

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/978,224
Filing Date	10/16/2001
First Named Inventor	Reuben Bahar
Art Unit	2143
Examiner Name	BILGRAMI, ASGHAR H.
Attorney Docket Number	6589-A-7

ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/ Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): First Amended Brief of Appellant, including copies of Choi, Flynn, and Bisbee patents.
<input type="text"/> Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Cahill, von Hellens & Glazer, P.L.C.		
Signature			
Printed name	Marvin A. Glazer		
Date	12/05/07	Reg. No.	28,801

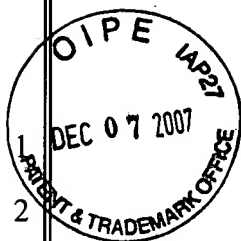
CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Marvin A. Glazer, Esq.	Date	12/05/07

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPL. NO.: 09/978,224

APPLICANT: REUBEN BAHAR

FILED: 02/13/2003

FOR: "METHOD AND SYSTEM
CONFIRMING PROPER
RECEIPT OF E-MAIL
TRANSMITTED VIA A
COMMUNICATIONS
NETWORK"

Art Unit 2143


Examiner: Asghar H. Bilgrami

Confirmation No. 4472

Attorney Docket No. 6589-7

Certificate of Transmission under 37 CFR 1.8

I hereby certify that this correspondence is being deposited on the date indicated below by first class mail, in the United States Postal Service addressed to: Commissioner of Patents,
P.O. Box 1450, Alexandria, VA 22313-1450


Marvin A. Glazer

Dec. 5, 2007
Date

FIRST AMENDED BRIEF OF APPELLANT

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This First Amended Brief of Appellant is being filed in response to the Notification of Non-Compliant Appeal Brief (Form PTOL-462) mailed November 16, 2007.

1 The Notification of Non-Compliant Appeal Brief indicated that the claims appendix did not
2 contain a “clean copy” of the appealed claims. By telephone conference held on December 3, 2007,
3 between the undersigned attorney and Patent Appeal Center Specialist Timothy Cole, it was
4 determined that the text of patent claims 215 and 251, as presented in the original Appeal Brief
5 filed on October 29, 2007, still included strike-out deletion and underline insertion markings.
6 Accordingly, in the present First Amended Appeal Brief, patent claims 215 and 251 have been
7 revised to be in “clean” form.

8 The Notification of Non-Compliant Appeal Brief also indicated that the original Appeal
9 Brief filed on October 29, 2007 did not “contain copies of the evidence submitted.” In this regard,
10 the “Evidence Appendix” included in the original Appeal Brief filed on October 29, 2007, recites
11 that copies of the patent references relied upon by the Examiner to reject the appealed claims,
12 namely, U.S. Pat. No. 6,629,131 (Choi); U.S. Pat. No. 6,618,747 (Flynn), and U.S. Pat. No.
13 5,748,738 (Bisbee) were attached to the original Appeal Brief. Nonetheless, during the telephone
14 conference held on December 3, 2007, between the undersigned attorney and Patent Appeal Center
15 Specialist Timothy Cole, Mr. Cole indicated that the original Appeal Brief filed on October 29,
16 2007 did not have such copies attached. Accordingly, copies of these three patents are attached to
17 this First Amended Appeal Brief immediately behind the Evidence Appendix, and just before the
18 concluding Related Proceedings Appendix.

19 This First Amended Appeal Brief is in support of the Notice of Appeal filed in the Patent
20 Office by the above-identified Applicant/Appellant on August 6, 2007, appealing the final rejection
21 of the Examiner dated June 6, 2007, finally rejecting claims 184-189, 191-213, 215-229, 231-234,
22 236-243, 248-255, 258-271, 279, 288-317, 327-340, and 346-348¹. A check in payment of the fee
23

24 ¹ In partial response to the final Office Action mailed June 6, 2007, Applicant canceled claims
25 155, 157-161, 163-182, 235, 244-247, 256-257, 272-278, 280-287, 318-326, and 341-345 by submitting
26 an Amendment After Final Office Action, without prejudice to the presentation of such claims in a
27 continuing application for further prosecution, in order to place the present application in better form
for purposes of appeal. The Examiner confirmed entry of such Amendment on September 6, 2007 via

1 of \$250.00 for filing an Appeal Brief, as set forth in § 41.20(b)(2) for a small entity, was already
2 forwarded to the Patent Office with the original Appeal Brief filed on October 29, 2007. The
3 Patent Office is hereby authorized to charge any additional fees required by this paper to Deposit
4 Account No. 03-0088.

5 This First Amended Appeal Brief sets forth the authorities and arguments on which
6 Appellant relies to maintain this appeal. A Claims Appendix, setting forth the text of the claims
7 involved in this appeal, is attached hereto. Also attached are appendices for evidence and related
8 proceedings.

9
10 **1. Real Party In Interest.**

11 The real party in interest is the applicant/inventor, namely, Reuben Bahar of West Hills,
12 California. The claimed invention has not been assigned or licensed.

13
14 **2. Related Appeals and Interferences.**

15 None.

16
17
18
19 **3. Status of Claims.**

20 None of the pending claims are allowed or objected to. All of claims 1-348 are either: 1)
21 rejected and being appealed; or 2) canceled, in accordance with the listing below:

22
23
24 _____
25 an Advisory Office Action. While preparing the original Appeal Brief, Applicant realized that
26 dependent claims 288-317 should also have been canceled, as they depend from canceled claims;
27 accordingly, on October 23, 2007, Applicant filed (via facsimile) a Supplemental Amendment After
Final Office Action canceling dependent claims 288-317.

<u>Claims</u>	<u>Status</u>
1-183	Canceled.
184-189	Rejected and being appealed.
190.	Canceled.
191-213	Rejected and being appealed.
214	Canceled.
215-229	Rejected and being appealed.
230	Canceled.
231-234	Rejected and being appealed.
235	Canceled.
236-243	Rejected and being appealed.
244-247	Canceled.
248-255	Rejected and being appealed.
256-257	Canceled.
258-271	Rejected and being appealed.
272-278	Canceled.
279	Rejected and being appealed.
280-326	Canceled.
327-340	Rejected and being appealed.
341-345	Canceled.
346-348	Rejected and being appealed.

4. Status of Amendments.

1 On July 30, 2007, Applicant filed an Amendment After Final Office Action. The entry of
2 the aforementioned amendment (which merely canceled additional claims) was confirmed by the
3 Examiner within an Advisory Office Action mailed on September 6, 2007.

4 While preparing the original Appeal Brief filed on October 29, 2007, Applicant realized that
5 dependent claims 288-317 should also have been canceled, since they all depend, directly or
6 indirectly, from canceled claims (either canceled claim 287 or canceled claim 272). Accordingly,
7 on October 23, 2007, Applicant filed (via facsimile) a Supplemental Amendment After Final Office
8 Action canceling dependent claims 288-317, without prejudice to the presentation of such claims in
9 a continuation patent application. It is not yet known whether the Examiner will enter such
10 Supplemental Amendment, though entry of such Supplemental Amendment would appear to be
11 proper pursuant to 37 C.F.R. §41.33(a). Accordingly, the Claims Appendix to this First Amended
12 Appeal Brief indicates that dependent claims 288-317 have been canceled.

13
14 **5. Summary of Claimed Subject Matter.**

15 Applicant has set forth below a concise explanation of the subject matter defined in each of
16 the independent claims (236, 248, 252, 258, 260, 264, and 268) involved in the appeal, including
17 references to the specification by page and line number, and to the drawings by reference
18 characters, where appropriate.

19
20 **Claim 236:**

21 Claim 236 recites a method for verifying whether an e-mail message 12 sent by a sending
22 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message
23 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications
24 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18). E-mail message 12 is delivered to a
25 designated recipient e-mail address. The recited method includes the step of detecting an access
26
27

1 event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts
2 the accessing party 20 to input recipient data (see spec. p. 27, lines 6-23) before allowing the access
3 to such email message by the accessing party 20; the aforementioned recipient data includes
4 identifying data related to the accessing party 20. The method of claim 236 also sends recipient
5 data back to sending party 10 for confirming proper delivery of e-mail message 12 (see spec. p. 23,
6 lines 3-14, and p. 31, lines 11-15).
7
8

9 Claim 248:

10 Claim 248 recites a system for verifying whether an e-mail message 12 sent by a sending
11 party 10 was accessed by an intended recipient. The system of claim 248 includes a sender
12 computer 11 connected to a communications network 13 and from which e-mail message 12 is
13 transmitted (see spec. p. 13, lines 16-18, and p. 14, lines 12-13). The system of claim 248 also
14 includes a recipient computer 14/21 connected to communications network 13 (see items 14 and 21
15 in Fig. 1, and see spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9);
16 the recipient computer 14/21 is capable of receiving e-mail message 12 and includes data storage
17 17/24 for storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17,
18 lines 10-19).
19
20

21 The system of claim 248 also includes software (e.g., executable attachment file 12' in Fig.
22 1) that is capable of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2); upon
23 detecting such access event, this software 12' prompts accessing party 20 to input recipient data
24 before allowing access to e-mail message 12 (see spec. p. 27, lines 6-23). The recipient data
25 inputted by accessing party 20 includes identifying data which identifies the accessing party 20 (e.g.,
26
27

1 see spec. p. 27, lines 13-17, and p. 29, lines 14-23) . The system of claim 248 also includes
2 “means” (e.g., software) for sending recipient data back to sending party 10 for confirming proper
3 delivery of e-mail message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and
4 4; also see, for example, spec. p. 19, lines 1-11).

6
7 Claim 252:

8 Claim 252 recites a system for verifying whether an e-mail message sent by a sending party
9 10 was accessed by an intended recipient. The system of claim 252 includes a sender computer 11
10 connected to a communications network 13 and from which e-mail message 12 is transmitted (see
11 spec. p. 13, lines 16-18, and p. 14, lines 12-13). The system of claim 252 also includes a recipient
12 computer 14/21 connected to communications network 13 (see items 14 and 21 in Fig. 1, and see
13 spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9); the recipient
14 computer 14/21 is capable of receiving e-mail message 12 and includes data storage 17/24 for
15 storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17, lines 10-19).

16
17
18 The system of claim 252 further includes a “means” for recognizing biometric attributes of
19 an individual (see spec. p. 29, line 14 through p. 30, line 23).

20 The system of claim 252 also includes software capable of detecting an access event (see
21 spec. p. 17, line 20, through p. 18, line 2) and identifying an individual through utilization of
22 inputted biometric attributes of said individual (see spec. p. 29, line 14 through p. 30, line 23).

23
24 Lastly, the system of claim 252 includes “means” (e.g., software) for sending data that
25 identifies the accessing party back to sending party 10 for confirming proper delivery of the e-mail
26
27

1 message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and 4; also see, for
2 example, spec. p. 19, lines 1-11).

3
4
5 Claim 258:

6 Claim 258 recites a method for verifying whether an e-mail message 12 sent by a sending
7 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message
8 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications
9 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to an e-mail
10 address. The recited method includes the step of detecting an access event (see spec. p. 17, line 20
11 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts the accessing party 20 to
12 input recipient data (see spec. p. 27, lines 6-23) before allowing the access to such email message
13 by the accessing party 20; the aforementioned recipient data includes identifying data associated
14 with the accessing party 20. The method of claim 258 also sends recipient data back to sending
15 party 10 for confirming proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p.
16 31, lines 11-15).

17
18
19
20 Claim 260:

21 Claim 260 recites a method for verifying whether an e-mail message 12 sent by a sending
22 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message
23 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications
24 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to a recipient e-
25 mail address. The recited method includes the step of detecting an access event (see spec. p. 17,
26
27

1 line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 260 includes
2 the further step of acquiring recipient data, wherein such recipient data is related to biometric
3 identification of the accessing party 20 (see spec. p. 29, line 14 through p. 30, line 23).
4

5 The method of claim 260 also sends recipient data back to sending party 10 for confirming
6 proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).
7

8 Claim 264:

9 Claim 264 recites a method for verifying whether an e-mail message 12 sent by a sending
10 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message
11 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications
12 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18). E-mail message 12 is delivered to
13 an e-mail address. The method of claim 264 includes the step of utilizing biometric identification
14 information to identify a recipient requesting access to the email message (see spec. p. 29, line 14
15 through p. 30, line 23).
16
17

18 The method of claim 264 further includes the step of detecting an access event (see spec. p.
19 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 264 also
20 sends recipient identification data back to sending party 10 for confirming proper delivery of the e-
21 mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).
22

23 Claim 268:

24 Claim 268 recites a method for verifying whether an e-mail message 12 sent by a sending
25 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message
26
27

1 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications
2 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to an e-mail
3 address. The method of claim 268 includes the further step of identifying a recipient requesting
4 access to e-mail message 12 using biometric identification information associated with such
5 recipient (see spec. p. 29, line 14 through p. 30, line 23).
6

7 The method of claim 268 further includes the step of detecting an access event (see spec. p.
8 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 268 also
9 sends recipient identification data back to sending party 10 for confirming proper delivery of the e-
10 mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).
11

12 13 **6. Grounds of Rejection to be Reviewed on Appeal:**

14 a. Did the Patent Examiner error in rejecting claims 184-189, 191-213, 215-229, 231-234,
15 236-243, 248-255, 258-271, 279, 327-340, and 346-348, as describing subject matter that would
16 have been obvious to those skilled in the art under 35 U.S.C. Section 103(a) based upon Choi (U.S.
17 Pat. No. 6,629,131), Flynn (U.S. Pat. No. 6,618,747), and Bisbee (U.S. Pat. No. 5,748,738)?
18
19

20 **7. Argument.**

21 **A. The Cited Prior Art.**

22 Choi (U.S. Patent No. 6,629,131):
23

24 The cited '131 patent to Choi describes a method for confirming receipt of an email
25 message. Choi's method assigns a unique code to an e-mail message sent by a sender, and records
26 the unique code in a database. This unique code is generated at the sender's end of the
27

1 transmission and is attached to the e-mail message as a "CGI executive program". Upon access of
2 the email message by the recipient, Choi's method sends the unique code that was attached to the
3 message back to the web server of the sender; this step is performed by the automatic execution of
4 the attached "CGI executive program" executed at the receiver's end when the e-mail message is
5 received by the receiver. A comparison is made of the unique code received from the CGI
6 executive program and the unique code previously recorded when the sender first sent the email
7 message. If the two codes are identical, then confirmation information is sent to the sender
8 indicating that the email message has been accessed.
9

10 Flynn (U.S. Patent No. 6,618,747):
11

12 The cited '747 patent to Flynn discloses a system wherein an intended recipient is notified
13 that an email message has been posted at a third party web host for such recipient. Notification of
14 the existence of the posted e-mail is communicated by the third party web host which sends an e-
15 mail message informing the recipient that an e-mail message is waiting for the recipient at a
16 specified third party web host URL. Included in this e-mail message is the third party URL address
17 where the posted message is located. If the intended recipient accesses the message, a confirmation
18 notice is sent to the sender to confirm that the message was downloaded. Flynn describes the URL
19 address at which the posted e-mail message is posted on the third party web host as a "unique call
20 address" (assigned by Flynn's Web Server 24) that provides access to an e-mail message stored at
21 such unique call address on the third party Web server. When the email message is downloaded by
22 the requesting party, Flynn's system sends a confirmation of receipt notice that includes the address
23 to which the email was downloaded, the time it was downloaded, and optionally, a compressed
24 copy of the original message.
25
26
27

1 Bisbee (U.S. Pat. No. 5,748,738):

2 The cited patent to Bisbee discloses a system for verifying the authenticity of the creator of
3 an electronic document. An authentication center provides third party verification that a document
4 is being transmitted by the originator of the document. Bisbee mentions the use by the
5 Certification Authority of personal identification information, such as biometric information (e.g.,
6 retina-, finger-, and voice-prints), to identify the document originator.
7

8
9 **B. The Examiner's Rejections:**

10 Within the final Office Action mailed June 6, 2007, the Patent Examiner finally rejected
11 claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-
12 348 under Section 103(a). The Examiner rejected such claims as describing subject matter
13 considered to be unpatentable over Choi (U.S. Pat. No. 6,629,131), Flynn (U.S. Pat. No.
14 6,618,747), and Bisbee (U.S. Pat. No. 5,748,738).
15

16
17
18 **C. The Cited Patents Do Not Render Obvious the Appealed Claims:**

19 Claim 236:

20 Claim 236 sets forth a method for verifying whether an e-mail sent by a sending party was
21 accessed by an intended recipient. The recited method includes the step of "detecting an access
22 event, and prompting the party associated with said access event to input recipient data prior to
23 allowing the requested access". Moreover, claim 236 states that the "recipient data" (which the
24 recipient must input before being allowed to access the e-mail message) includes "identifying data
25
26
27

1 related to the party associated with said requested access”. Claim 236 further recites that such
2 “recipient data” is then sent to confirm proper delivery of the e-mail message.

3 The Patent Examiner rejected claim 236 within paragraph 4 on page 2 of the final Office
4 Action mailed June 6, 2007. Within such paragraph 4, the Patent Examiner stated the following:
5

6 “4. As per claims 236, Choi disclosed a method for verifying whether an e-mail sent
7 by a sending party was accessed by an intended recipient, said method comprising a) storing
8 recipient data pertaining to an actual recipient of e-mail in a data file, said stored data file
9 containing identifying data that identifies actual e-mail recipient and further being
10 associated with actual recipient’s email address (col. 1, lines 36-53); b) transmitting an e-
11 mail from a send computer to an intended recipient, the sender computer being connected to
12 a communications network; c) delivering said e-mail to a recipient e-mail address (col. 2,
13 lines 59-67). However, Choi did not explicitly disclose d) detecting an access event, and
14 discovering stored data file that is associated with said actual recipient’s e-mail address and
15 (e) sending identifying data contained in said discovered data file for confirming proper
delivery of said e-mail.”

16 Within the Examiner’s above-quoted remarks, the Examiner did not address the requirement in
17 claim 236 for the step of “detecting an access event, *and prompting the party associated with said*
18 *access event to input recipient data prior to allowing the requested access*”. Neither Choi nor
19 Flynn discloses or suggests this aspect of applicant’s invention.

20 The only portion of the final Office Action in which the Examiner addressed the
21 requirement in claim 236 for “detecting an access event, and prompting the party associated with
22 said access event to input recipient data prior to allowing the requested access” is in paragraph 17
23 on page 7 of the final Office Action. In paragraph 17 of the final Office Action, the Patent
24 Examiner stated the following:
25
26
27

1 “17. Applicant argued that neither Flynn nor Choi, disclose or suggest prompting a
2 party requesting to access an e-mail to enter recipient data after detecting an access event.

3 As to applicant’s argument examiner introduced Bisbee, which prompts the user to
4 enter its recipient data (I.E. biometric, password information) to access the event (checking
5 the e-mail message). Please see rejection on line 4 [*sic paragraph 4 ?*] of this office
6 action.”

7 As will be shown below, the Patent Examiner’s contention that Bisbee prompts a user to enter
8 recipient data in order to access an e-mail message is incorrect, and unsupported by the Bisbee
9 disclosure.

10 The Background section of Bisbee (set forth in columns 1 and 2 of the Bisbee patent) is
11 concerned with the problem of document alteration/document forgery. Later, (in col. 6), Bisbee
12 talks about preventing the originator from denying the authenticity of the document. These remarks
13 relate to the identity of the originator of the document, and not to an individual seeking access to
14 such document.

15 Bisbee proposes that the true identity of the document originator can be verified by use of a
16 “Token”, as Bisbee explains at col. 4, lines 35-49, as follows:
17

18 “ As described below, the public/private key is advantageously delivered in the form
19 of a Token such as an electronic circuit card conforming to the standards of the PC Memory
20 Card Interface Association (a PCMCIA card or PC Card) **for use in the originator's**
21 **computer**. In general a Token is a portable transfer device that is used for transporting
22 keys, or parts of keys. It will be understood that PC Cards are just one form of delivery
23 mechanism for public/private keys for Applicant's DAS; other kinds of Tokens may also be
24 used, such as floppy diskettes and Smart Cards. To ensure reliable delivery a service such
25 as the bonded courier services commonly used to ferry securities between parties could be
26 used **to deliver the media to the document originator**.” (Emphasis added)
27

1 At col. 4, line 61, through col. 5, line 4, the Bisbee specification states the following:

2 “ In an additional aspect of Applicant's invention, the public/private key is only
3 effective when it is used in conjunction with a certificate and personal identification
4 information such as the *recipient's* biometric information (e.g., retina-, finger-, and voice-
5 prints) or a personal identification number (PIN) that is assigned to the *recipient* of the card
6 by the Certification Authority and that may be delivered separate from the originator's card.
7 Any subsequent transmitter of the document who is required to digitally sign or encrypt the
8 document would similarly be provided with a respective card and personal identification
9 information.”

10 Within the text quoted immediately above, Bisbee uses the word "*recipient*" to mean the recipient
11 of the Token "for use in the originator's computer" (see col. 4, lines 35-49, which describe delivery
12 of the Token to the "document originator"). See also col. 4, line 60 (".. the reliable delivery of the
13 Token to the authorized recipient.").

14 Thus, when Bisbee speaks of "personal identification information such as the *recipient's*
15 biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number
16 (PIN) that is assigned *to the recipient of the card* by the Certification Authority", Bisbee is
17 referring to the "recipient" of the Token and/or PC Card (i.e., the document transmitter/originator),
18 and not the intended recipient of the document requiring authentication. Indeed, the only portion of
19 the Bisbee specification that actually discusses the issue of who has the right to access a document
20 is in col. 10, lines 17-22; that portion of Bisbee is very vague, and it certainly does not disclose or
21 suggest the step of prompting the accessing party to input recipient data after detecting an access
22 event, and prior to allowing the requested access.

25 Accordingly, the Examiner's rejection of claim 236 is not supported by the cited references
26 and should be reversed.

1 Claim 248:

2 Claim 248 recites a system for verifying whether e-mail sent by a sending party was
3 accessed by an intended recipient, wherein such system includes, among other things, a recipient
4 computer connected to a communications network and being capable of receiving and storing a
5 transmitted e-mail message, and software capable of detecting an access event, "... said software
6 prompts the party associated with said access event to input recipient data prior to allowing the
7 requested access".
8

9 Once again, the Patent Examiner's rejection of claim 248 is set forth in paragraph 4 of the
10 final Office Action, but such paragraph 4 fails to address the requirement within claim 248 for
11 software capable of detecting an access event and thereafter prompting the accessing party to input
12 recipient data prior to allowing the requested access.
13

14 In addition, for the reasons explained above relative to claim 236, the Examiner's remarks
15 in paragraph 17 of the final Office Action, based upon Bisbee, fail to demonstrate that Bisbee
16 teaches or suggests software capable of detecting an access event and thereafter prompting the
17 accessing party to input recipient data prior to allowing the requested access.
18

19 Accordingly, the Examiner's rejection of claim 248 is not supported by the cited references
20 and should be reversed.
21

22 Claim 252:

23 Claim 252 recites a system for verifying whether e-mail sent by a sending party was
24 accessed by an intended recipient, the system including, among other things, a recipient computer
25 connected to a communications network and being capable of receiving and storing a transmitted e-
26
27

1 mail message; “biometric identification means” for recognizing biometric attributes of an
2 individual; software capable of detecting an access event and identifying an individual through
3 utilization of inputted biometric attributes of said individual; and “ means” for sending data that
4 identifies said individual for confirming proper delivery of said e-mail.
5

6 The Examiner sets forth the basis of the rejection of claim 252 in paragraph 4 of the final
7 Office Action. While the Examiner concedes that neither Choi nor Flynn explicitly disclose
8 detecting an individual by utilizing inputted biometric attributes of an individual, the Examiner
9 contends that “Bisbee disclosed detecting an individual through utilization of inputted biometric
10 attributes of said individual (col. 1, lines 37-51 & col. 4, lines 36-67).” The Examiner concludes
11 that “it would have been obvious ... to have incorporated detecting an accessing individual through
12 utilization of biometric attributes as disclosed by Bisbee ... ”.
13

14 However, the Examiner’s arguments are not supported by the Bisbee reference. The portion
15 of Bisbee’s specification noted by the Examiner in col. 1 (lines 37-51) are directed to the problem
16 of authenticating the “transferor” and/or “document’s originator”. Likewise, as applicant has
17 explained above, the portion of Bisbee’s specification appearing in col. 4, lines 36-67, is directed to
18 authenticating the document’s originator, and not a subsequent recipient of the document.
19

20 Accordingly, the Examiner’s proposed combination of Bisbee with Choi and Flynn
21 nonetheless fails to provide, or suggest, the invention recited in claim 252.
22

23
24 Claim 258:

25 Claim 258 recites a method for verifying whether an e-mail sent by a sending party was
26 accessed by an intended recipient. The preamble and steps a) and d) of claim 258 are identical to
27

1 method claim 236 discussed above. Step b) of claim 258 differs from step b) of claim 236 only in
2 that claim 258 is less specific about where the email message is delivered [“delivering said e-mail
3 to an e-mail address” (claim 258) versus “delivering said e-mail to a recipient e-mail address”
4 (claim 236)].
5

6 The differences between step c) of claim 258 and step c) recited in claim 236 are
7 highlighted in the table below:

8 Claim 258	9 Claim 236
10 c) detecting an access event, and 11 prompting the party 12 <i>that requested said access</i> 13 to input recipient data prior to allowing the 14 requested access, said recipient data including 15 identifying data 16 <i>that is associated with the party that</i> <i>requested</i> said access; and	c) detecting an access event, and prompting the party <i>associated with said access event</i> to input recipient data prior to allowing the requested access, said recipient data including identifying data <i>related to the party associated with said</i> <i>requested</i> access; and

17
18 The Examiner’s asserted basis for rejecting claim 258 is identical to the Examiner’s asserted basis
19 for rejecting claim 236 already discussed above. Applicant’s remarks, set forth above and directed
20 to rejected claim 236, apply with equal force relative to the rejection of claim 258. The Patent
21 Examiner’s contention that Bisbee prompts a user to enter recipient data in order to access an e-
22 mail message is incorrect, and the rejection of claim 258 should be reversed.
23
24
25
26
27

1 Claim 260:

2 Claim 260 recites a method for verifying whether e-mail sent by a sending party was
3 accessed by an intended recipient, and includes, *inter alia*, the steps of detecting an access event;
4 acquiring recipient data that is related to biometric identification of the recipient; and sending
5 recipient data for confirming proper delivery of said e-mail. The Examiner's rejection of claim 260
6 is set forth in paragraph 4 of the final Office Action. On page 3 of the final Office Action, the
7 Examiner concedes that the cited patents to Flynn and Choi fail to disclose detecting the identity of
8 an individual through utilization of inputted biometric attributes of said individual. The Examiner
9 contends that it would have been obvious to those skilled in the art to apply Bisbee's teachings
10 regarding biometric attributes to identify the party who received an email message.
11

12
13 As noted above, Bisbee's discussion of "personal identification information such as the
14 *recipient's* biometric information (e.g., retina-, finger-, and voice-prints) ..." refers to the party who
15 originates and/or transmits a document, who is a "recipient" of the Token and/or PC Card used to
16 authenticate the sender of the document. Bisbee never states or suggests that biometric
17 information might be used to identify a party receiving such document.
18

19 Accordingly, the Examiner's proposed combination of Bisbee with Choi and Flynn fails to
20 render obvious the subject matter recited in claim 260, and the Examiner's rejection should
21 therefore be reversed.
22

23 Claim 264:

24
25 Claim 264 recites a method for verifying whether e-mail sent by a sending party was
26 accessed by an intended recipient, including, among others, the steps of identifying a recipient
27

1 utilizing biometric identification; detecting an access event; and sending data that identifies said
2 recipient for confirming proper delivery of said e-mail. The Examiner's rejection of claim 264 is
3 set forth in paragraph 4 of the final Office Action.
4

5 As noted in regard to claim 260, the Examiner has conceded (see page 3 of the final Office
6 Action) that the cited patents to Flynn and Choi fail to disclose detecting the identity of an
7 individual through utilization of inputted biometric attributes of said individual. Nonetheless, the
8 Examiner contends that it would have been obvious to those skilled in the art, based upon Bisbee,
9 to utilize biometric attributes to identify the party who received an email message.
10

11 The applicant has already pointed out that Bisbee's disclosure teaches the use of biometric
12 information only to identify the originator/sender of a document, and that Bisbee's disclosure fails
13 to disclose or suggest the use of biometric information to identify a party receiving a document.
14 Therefore, the Examiner's proposed combination of Bisbee with Choi and Flynn does not suggest
15 the subject matter recited in claim 264, and the Examiner's rejection should accordingly be
16 reversed.
17

18 Claim 268:

19 Claim 268 recites a method for verifying whether an e-mail sent by a sending party was
20 accessed by an intended recipient. The preamble and steps a), b), d) and e) of claim 268 are
21 identical to method claim 264 discussed above. The differences between step c) of claim 268 and
22 step c) recited in claim 264 are highlighted in the table below:
23
24
25
26
27

Claim 268	Claim 264
c) identifying a recipient <i>in association with</i> biometric identification;	c) identifying a recipient <i>utilizing</i> biometric identification;

Notwithstanding the differences in the wording of step c) as between claims 268 and 264, the cited Bisbee patent does not make use of any biometric information to identify the recipient of a document. Thus, the rejection of claim 268 should be reversed for essentially the same reasons as explained above in regard to independent claims 260 and 264.

8. Conclusion:

Accordingly, Appellant submits that the appealed independent claims 236, 248, 252, 258, 260, 264, and 268, and those appealed claims dependent therefrom, define subject matter that is patentably distinguishable over the applied prior art, and requests the Board to reverse the rejection of appealed claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.



Marvin A. Glazer
Registration No. 28,801

155 Park One
2141 East Highland Avenue
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6589-A-7

1 **CLAIMS APPENDIX (Claims Involved In The Appeal)**

2

3 1. - 183. Canceled.

4

5 184. The method as recited in claim 258 wherein said step of sending recipient data for

6 confirming proper delivery of said e-mail includes the steps of:

7 a) generating a confirmation of receipt notice wherein the inputted recipient data is included with

8 said confirmation of receipt notice; and

9 b) sending said confirmation of receipt notice, wherein the inputted recipient data included with

10 said confirmation of receipt notice can be compared to information associated with said intended

11 recipient in order to verify whether the e-mail was accessed by the intended recipient.

12

13 185. The method as in claim 236, wherein said access event comprises access of said e-mail

14 that was delivered to said recipient e-mail address.

15

16 186. The method as in claim 236, wherein said access event comprises access of an e-mail

17 account associated with said recipient e-mail address.

18

19 187. The method as in claim 236, wherein said access event comprises activation of an e-mail

20 processing software associated with said recipient e-mail address.

21

22 188. The method as in claim 236, wherein the step of transmitting an e-mail from a sender

23 computer includes attaching an executable attachment file in conjunction with the e-mail, the

24 executable attachment file having a first module for prompting the party who requested said access

25 event to enter recipient data; and

26

27

1 and wherein the step of detecting an access event includes the step of executing the first
2 module of the executable attachment file.

3
4 189. The method as in claim 188, wherein the executable attachment file has a second module
5 transmitted and delivered therewith, the second module for detecting the access event, and further
6 comprising the step of automatically executing the second module upon delivery of the attachment
7 file to the recipient e-mail address.

8
9 190. *Canceled.*

10
11 191. The method as in claim 236, wherein said recipient e-mail address is associated with a
12 recipient computer.

13
14 192. The method as in claim 191, wherein said recipient computer is a server of a service
15 provider.

16
17 193. The method as in claim 191, wherein said recipient computer is a user system that is
18 directly accessible by a recipient, said user system including electronic mail processing software.

19 194. The method as in claim 236 , wherein said inputted recipient data pertains to
20 alphanumeric text identification, biometric identification, password identification, a computer
21 generated user code, or a combination thereof.

22
23 195. The method as in claim 236, wherein said inputted recipient data comprises identity
24 information that identifies an individual.

1 196. The method as in claim 195, wherein said identity information pertains to biometric
2 identification.

3
4 197. The method as in claim 196 further comprising the step of recognizing biometric
5 attributes of an individual.

6
7 198. The method as in claim 195, wherein said identity information includes alphanumeric
8 text identification information.

9
10 199. The method as in claim 236 , wherein said inputted recipient data comprises information
11 that identifies a business.

12
13 200. The method as in claim 236, wherein said inputted recipient data comprises information
14 that identifies an organization.

15
16 201. The method as in claim 236 , wherein said inputted recipient data comprises a computer
17 generated user code.

18
19 202. The method as in claim 236 further including the step of sending access event data of
20 attendant conditions of said access event.

21
22 203. The method as in claim 236 , wherein said recipient is an individual.

23
24 204. The method as in claim 236, wherein said recipient is a business.

25
26 205. The method as in claim 236, wherein said recipient is an organization.

1 206. The method as in claim 236, wherein said inputted recipient data is used to verify proper
2 delivery of legal documents.

3
4 207. The method as in claim 236, wherein said inputted recipient data is used to verify
5 proper delivery of confidential documents.

6
7 208. The method recited by claim 260 wherein said step of sending recipient data for
8 confirming proper delivery of said e-mail includes the steps of:

9 a) generating a confirmation of receipt notice wherein the acquired recipient data is
10 included with said confirmation of receipt notice; and

11 b) sending said confirmation of receipt notice, wherein the acquired recipient data
12 contained with said confirmation of receipt notice can be compared to information associated with
13 said intended recipient in order to verify whether the email was accessed by the intended recipient.

14
15 209. The method as in claim 260, wherein said access event comprises access of said e-mail
16 that was delivered to said recipient e-mail address.

17
18 210. The method as in claim 260, wherein said access event comprises access of an e-mail
19 account associated with said recipient e-mail address.

20
21 211. The method as in claim 260, wherein said access event comprises activation of e-mail
22 processing software associated with said recipient e-mail address.

23
24 212. The method as in claim 260, wherein the step of transmitting an e-mail from a sender
25 computer includes attaching an executable attachment file in conjunction with the e-mail, the
26

1 executable attachment file having a first module for acquiring recipient data that is related to
2 biometric identification of the recipient, and

3 wherein the step of detecting an access event includes the step of executing the first module
4 of the executable attachment file.

5
6
7 213. The method as in claim 212, wherein the executable attachment file has a second module
8 transmitted and delivered therewith, the second module for detecting the access event, and further
9 comprising the step of:

10 automatically executing the second module upon delivery of the attachment file to the
11 recipient e-mail address.

12
13 214. Canceled.

14
15 215. The method as in claim 260, wherein said recipient e-mail address is associated with
16 a recipient computer.

17
18 216. The method as in claim 215, wherein said recipient computer is a server of a service
19 provider that is capable of receiving e-mail.

20
21 217. The method as in claim 215, wherein said recipient computer is a user system that is
22 directly accessible by the recipient, said user system including electronic mail processing software
23 and being capable of receiving e-mail.

24
25 218. The method as in claim 260, wherein said acquired recipient data is related to a
26 biometric imprint, alphanumeric text identification, password identification, a computer generated

1 user code, or a combination thereof.

2
3 219. The method as in claim 260, wherein said acquired recipient data comprises identity
4 information that identifies an individual.

5
6 220. The method as in claim 260 further comprising means for recognizing biometric
7 attributes of an individual.

8
9 221. The method as in claim 260, wherein said acquired recipient data comprises
10 information that identifies a business.

11
12 222. The method as in claim 260, wherein said acquired recipient data comprises
13 information that identifies an organization.

14
15 223. The method as in claim 260, wherein said acquired recipient data comprises a
16 computer generated user code.

17
18 224. The method as in claim 260 further including the step of sending access event data
19 of conditions attendant said access event.

20
21 225. The method as in claim 260, wherein said recipient is an individual.

22
23 226. The method as in claim 260, wherein said recipient is a business.

24
25 227. The method as in claim 260, wherein said recipient is an organization.

1 228. The method as in claim 260, wherein said sent recipient data is used to verify proper
2 delivery of legal documents.

3
4 229. The method as in claim 260, wherein said sent recipient data is used to verify proper
5 delivery of confidential documents.

6
7 230. Canceled.

8
9 231. The method as in claim 260, wherein said recipient data is acquired as a requisite
10 condition for permitting access to said delivered e-mail.

11
12 232. The method as in claim 260, wherein said recipient data is acquired as a requisite
13 condition for permitting access to said recipient e-mail address.

14
15 233. The method as in claim 260, wherein said recipient data is acquired as a requisite
16 condition for operating a remote user computer, said remote user computer being operable to gain
17 access to said recipient e-mail address.

18
19 234. The method as in claim 260, wherein said recipient data is comprised of
20 alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute
21 of said recipient.

22
23 235. Canceled.

24
25 236. A method for verifying whether an e-mail sent by a sending party was accessed by
26 an intended recipient, said method comprising:

- a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;
- b) delivering said e-mail to a recipient e-mail address;
- c) detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access, said recipient data including identifying data related to the party associated with said requested access; and
- d) sending recipient data for confirming proper delivery of said e-mail.

237. The method recited by claim 264 wherein the step of sending data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of :

- a) generating a confirmation of receipt notice wherein the data that identifies the recipient is included with said confirmation of receipt notice; and
- b) sending said confirmation of receipt notice, wherein the data that identifies the recipient that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

238. The method as in claim 264, wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239. The method as in claim 264, wherein the data that identifies said recipient is comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one biometric attribute of said recipient.

1 240. The method as in claim 264 further including the step of recognizing biometric
2 attributes of an individual.

3 241. The method as in claim 264, wherein said data that identifies said recipient
4 comprises identity information that identifies an individual.

5
6 242. The method as in claim 264, wherein said data that identifies said recipient
7 comprises information that identifies a business.

8
9 243. The method as in claim 264, wherein said data that identifies said recipient
10 comprises information that identifies an organization.

11
12 244. - 247. Canceled.

13
14 248. A system for verifying whether e-mail sent by a sending party was accessed by an
15 intended recipient, said system comprising:

16 a) a sender computer connected to a communications network and from which an e-
17 mail is transmitted;

18 b) a recipient computer connected to said communications network, said recipient
19 computer capable of receiving said transmitted e-mail and further having data storage means for
20 storing said received e-mail;

21 c) software capable of detecting an access event, wherein, upon detecting said access
22 event, said software prompts the party associated with said access event to input recipient data prior
23 to allowing the requested access, said recipient data comprising identifying data related to the party
24 associated with said requested access; and

25 d) means for sending recipient data for confirming proper delivery of said e-mail.
26
27

1 249. The system as in claim 248, wherein said access event comprises access of a delivered e-
2 mail.

3
4 250. The system as in claim 248, wherein said access event comprises access of an e-mail
5 account associated with the e-mail address to which said e-mail was delivered.

6
7 251. The system as in claim 248, wherein said access event comprises activation of e-mail
8 processing software associated with the e-mail address to which said e-mail was delivered.

9
10 252. A system for verifying whether e-mail sent by a sending party was accessed by an
11 intended recipient, said system comprising:

12 a) a sender computer connected to a communications network and from which an e-mail is
13 transmitted;

14 b) a recipient computer connected to said communications network, said recipient
15 computer being capable of receiving said transmitted e-mail and further having data storage means
16 for storing said received e-mail;

17 c) biometric identification means for recognizing biometric attributes of an individual;

18 d) software capable of detecting an access event and identifying an individual through
19 utilization of inputted biometric attributes of said individual; and

20 e) means for sending data that identifies said individual for confirming proper delivery of
21 said e-mail.

22
23 253. The system as in claim 252, wherein said access event comprises access of a
24 delivered e-mail.

1 254. The system as in claim 252, wherein said access event comprises access of an e-mail
2 account associated with the e-mail address to which said e-mail was delivered.

3
4 255. The system as in claim 252, wherein said access event comprises activation of the e-mail
5 processing software associated with the e-mail address to which said e-mail was delivered.

6
7 256. - 257. Canceled.

8
9 258. A method for verifying whether an e-mail sent by a sending party was accessed by an
10 intended recipient, said method comprising:

11 a) transmitting an e-mail from a sender computer to an intended recipient, the sender
12 computer being connected to a communications network;

13 b) delivering said e-mail to an e-mail address;

14 c) detecting an access event, and prompting the party that requested said access to input
15 recipient data prior to allowing the requested access, said recipient data including identifying data
16 that is associated with the party that requested said access; and

17 d) sending recipient data for confirming proper delivery of said e-mail.

18
19 259. The method recited by claim 236 wherein said step of sending recipient data for confirming
20 proper delivery of said e-mail includes the steps of:

21 a) generating a confirmation of receipt notice wherein the inputted recipient data is included
22 with said confirmation of receipt notice; and

23 b) sending said confirmation of receipt notice, wherein the inputted recipient data included
24 with said confirmation of receipt notice can be compared to information associated with said
25 intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

1 260. A method for verifying whether e-mail sent by a sending party was accessed by an
2 intended recipient, said method comprising:

- 3 a) transmitting an e-mail from a sender computer to an intended recipient, the sender
4 computer being connected to a communications network;
5 b) delivering said e-mail to a recipient e-mail address;
6 c) detecting an access event;
7 d) acquiring recipient data that is related to biometric identification of the recipient; and
8 e) sending recipient data for confirming proper delivery of said e-mail.
9

10 261. The method as recited in claim 260 wherein said recipient data is acquired prior to said
11 access event.
12

13 262. The method as recited in claim 260 wherein said recipient data is acquired after said access
14 event.
15

16 263. The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.
17

18 264. A method for verifying whether e-mail sent by a sending party was accessed by an
19 intended recipient, said method comprising:

- 20 a) transmitting an e-mail from a sender computer to an intended recipient, the sender
21 computer being connected to a communications network;
22 b) delivering said e-mail to an e-mail address;
23 c) identifying a recipient utilizing biometric identification;
24 d) detecting an access event; and
25 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.
26
27

1 265. The method as recited in claim 264 wherein said recipient is identified prior to said access event.

2
3 266. The method as recited in claim 264 wherein said recipient is identified after said access
4 event.

5
6 267. The method as recited in claim 264 wherein said data that identifies said recipient is sent to
7 an e-mail address.

8
9 268. A method for verifying whether e-mail sent by a sending party was accessed by an intended
10 recipient, said method comprising:

- 11 a) transmitting an e-mail from a sender computer to an intended recipient, the sender
12 computer being connected to a communications network;
13 b) delivering said e-mail to an e-mail address;
14 c) identifying a recipient in association with biometric identification;
15 d) detecting an access event; and
16 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

17
18 269. The method as in claim 268 wherein said recipient is identified prior to said access event.

19
20 270. The method as in claim 268 wherein said recipient is identified after said access event.

21
22 271. The method as in claim 268 wherein said data that identifies said recipient is sent to an e-
23 mail address.

24
25 272. - 278. Canceled.

1 279. The system as in claim 252, wherein said data that identifies said individual for confirming
2 proper delivery of said e-mail is sent to an e-mail address.

3
4 280. - 326. Canceled.

5
6 327. The method as in claim 236, wherein said recipient data for confirming proper delivery of
7 said e-mail is sent to an e-mail address.

8
9 328. The method as in claim 236, wherein a remote user computer may be used to gain remote
10 access to said recipient e-mail address.

11
12 329. The method as in claim 236 wherein the party that is associated with said access event is
13 an individual.

14
15 330. The method as in claim 236 wherein the party that is associated with said access event is a
16 business.

17
18 331. The method as in claim 236 wherein the party that is associated with said access event is
19 an organization.

20
21 332. The method as in claim 258 wherein said recipient data for confirming proper delivery of
22 said e-mail is sent to an e-mail address.

23
24 333. The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-
25 mail address.

1 334. The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric
2 text identification, biometric identification, password identification, a computer generated user
3 code, or a combination thereof.

4
5 335. The method as in claim 208, wherein said confirmation of receipt notice is sent to an e-
6 mail address.

7
8 336. The method as in claim 260, wherein a remote user computer may be used to gain remote
9 access to said recipient e-mail address.

10
11 337. The method as in claim 219, wherein said identity information includes alphanumeric text
12 identification.

13
14 338. The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-
15 mail address.

16
17 339. The method as in claim 268, wherein said data that identifies said recipient is related to a
18 biometric imprint, alphanumeric text identification, password identification, a computer generated
19 user code, or a combination thereof.

20
21 340. The method as in claim 268 further comprising the step of recognizing biometric attributes
22 of an individual.

23
24 341. - 345. Canceled.

1 346. The system as in claim 248, wherein said recipient data for confirming proper delivery of
2 said e-mail is sent to an e-mail address.

3
4 347. The system as in claim 252, wherein said individual is identified prior to said access event.

5
6 348. The system as in claim 252, wherein said individual is identified after said access event.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

1 **EVIDENCE APPENDIX**

2 In regard to this Appeal, Appellant does not rely upon any evidence submitted pursuant to
3 37 C.F.R. §§ 1.130, 1.131 or 1.132.

4 The Patent Examiner has relied upon U.S. Pat. No. 6,629,131 (Choi); U.S. Pat. No.
5 6,618,747 (Flynn), and U.S. Pat. No. 5,748,738 (Bisbee), and Appellant has included remarks in the
6 foregoing First Amended Appeal Brief directed to such patent references. Accordingly, copies of
7 the Choi, Flynn, and Bisbee patents are attached hereto for the convenience of the Board.

Fig. 1

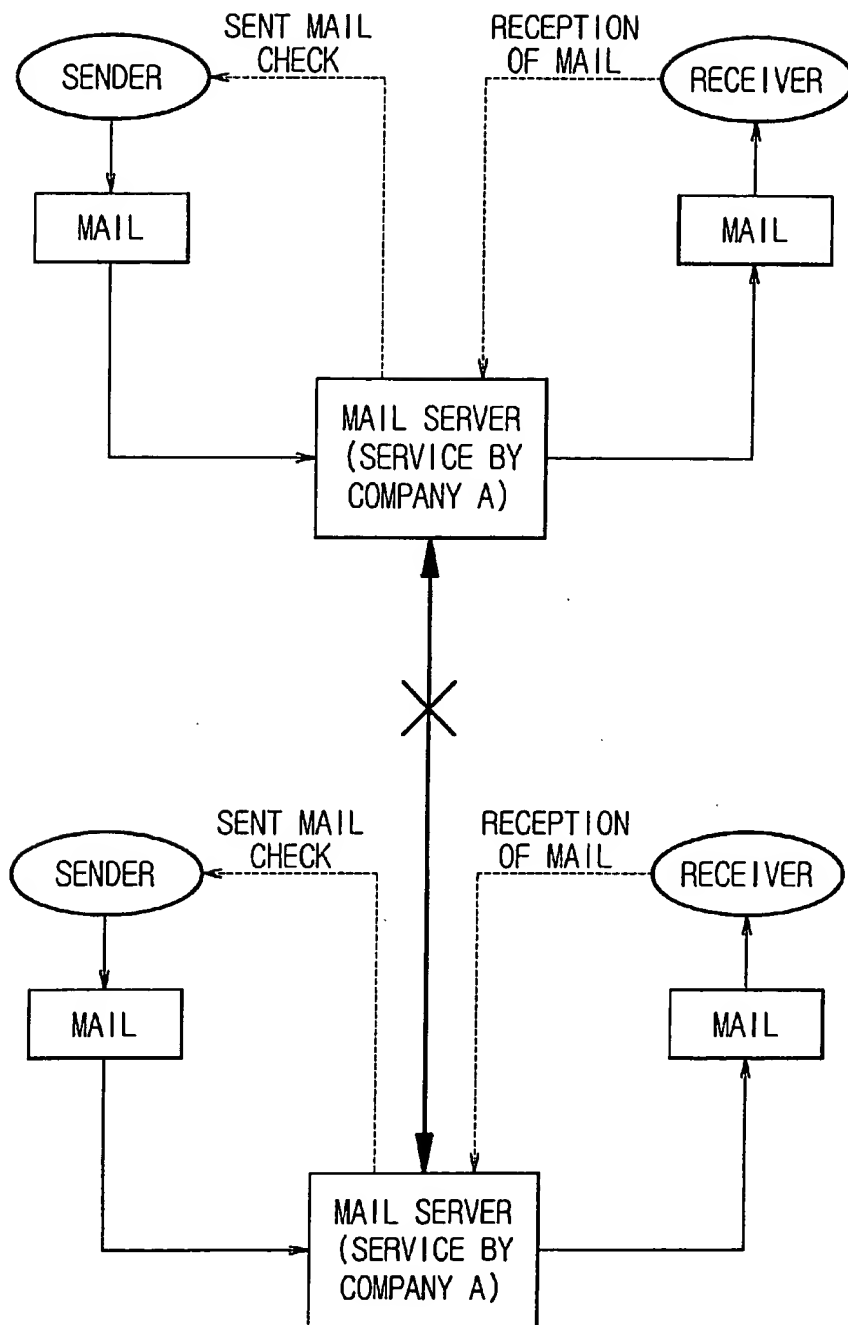


Fig.2

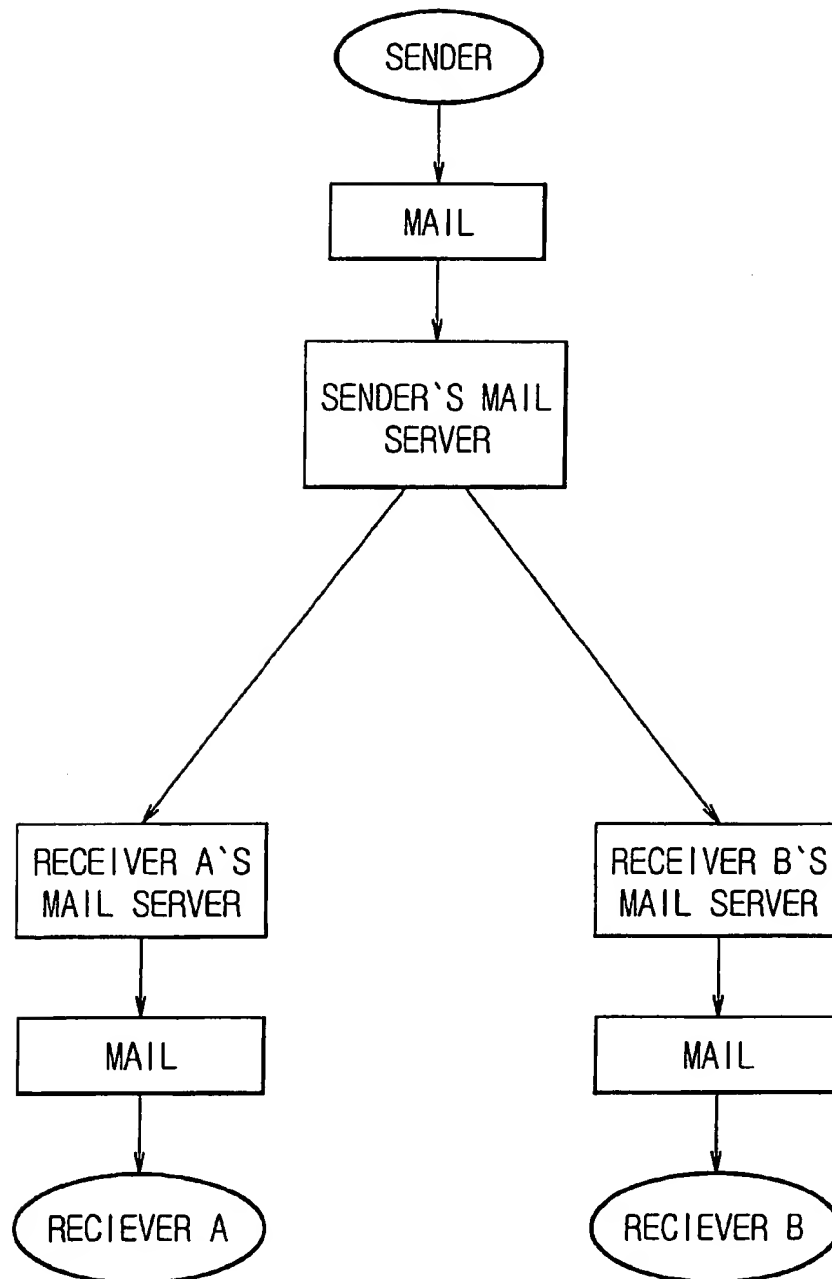


Fig.3

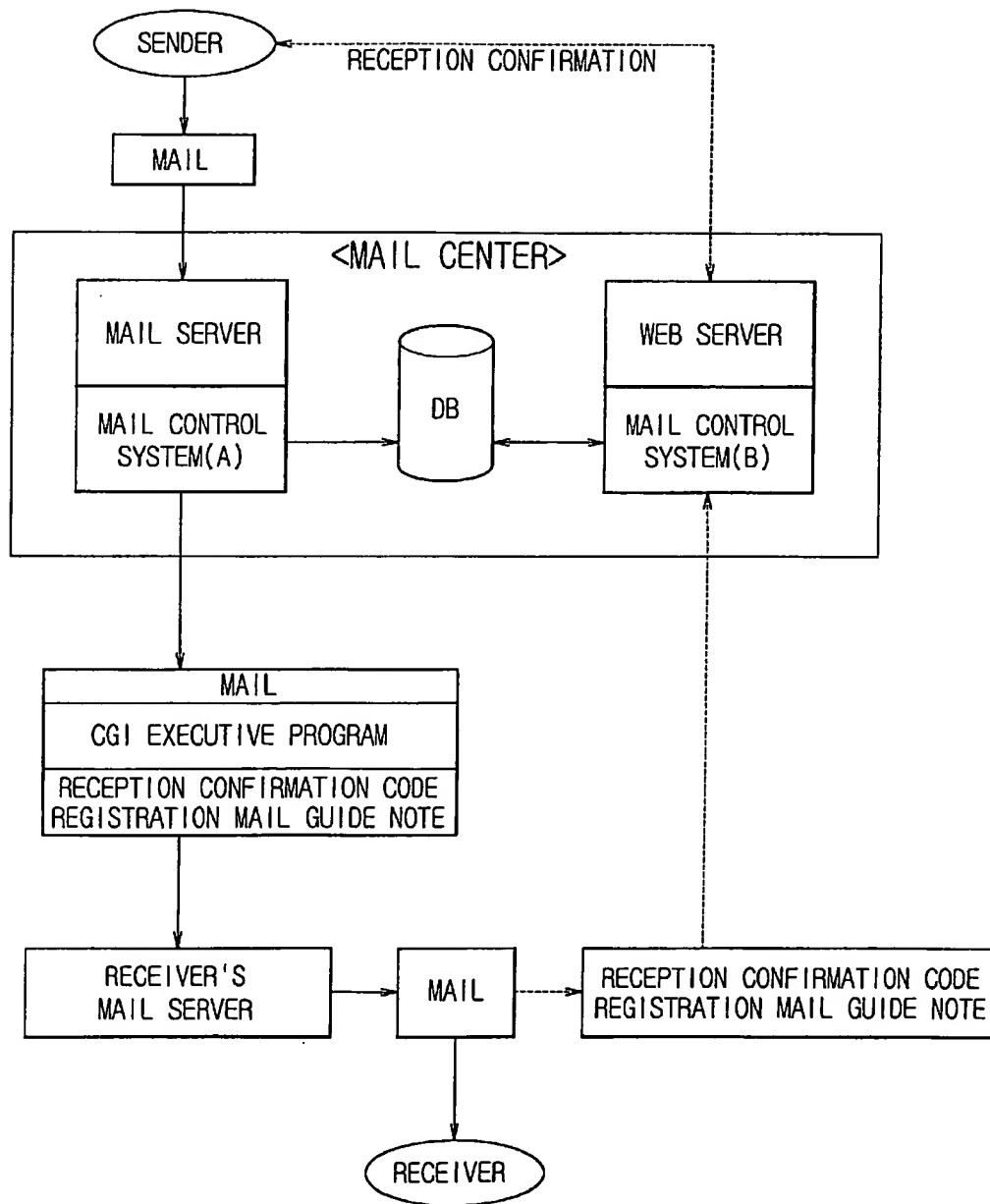


Fig.4

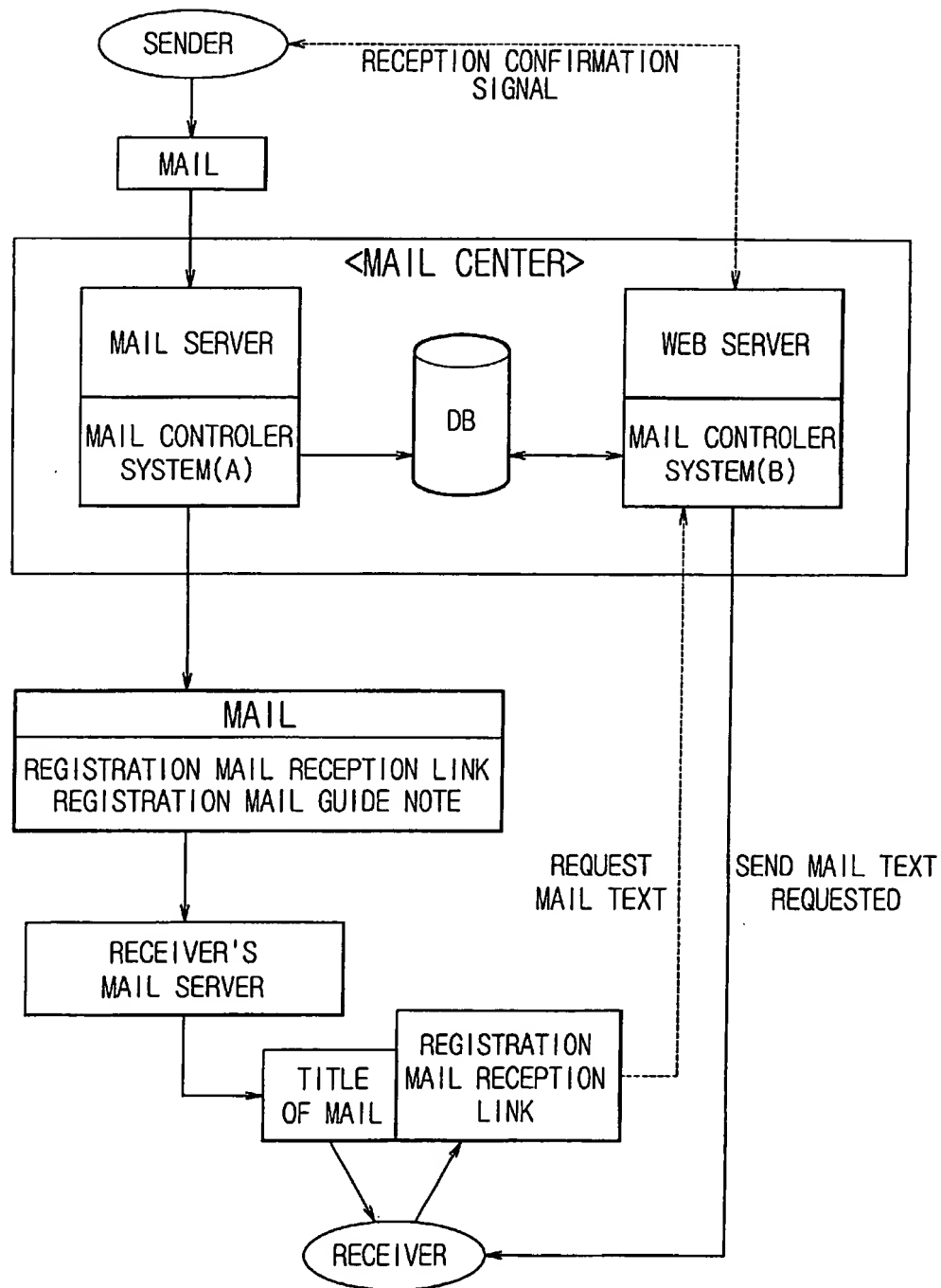
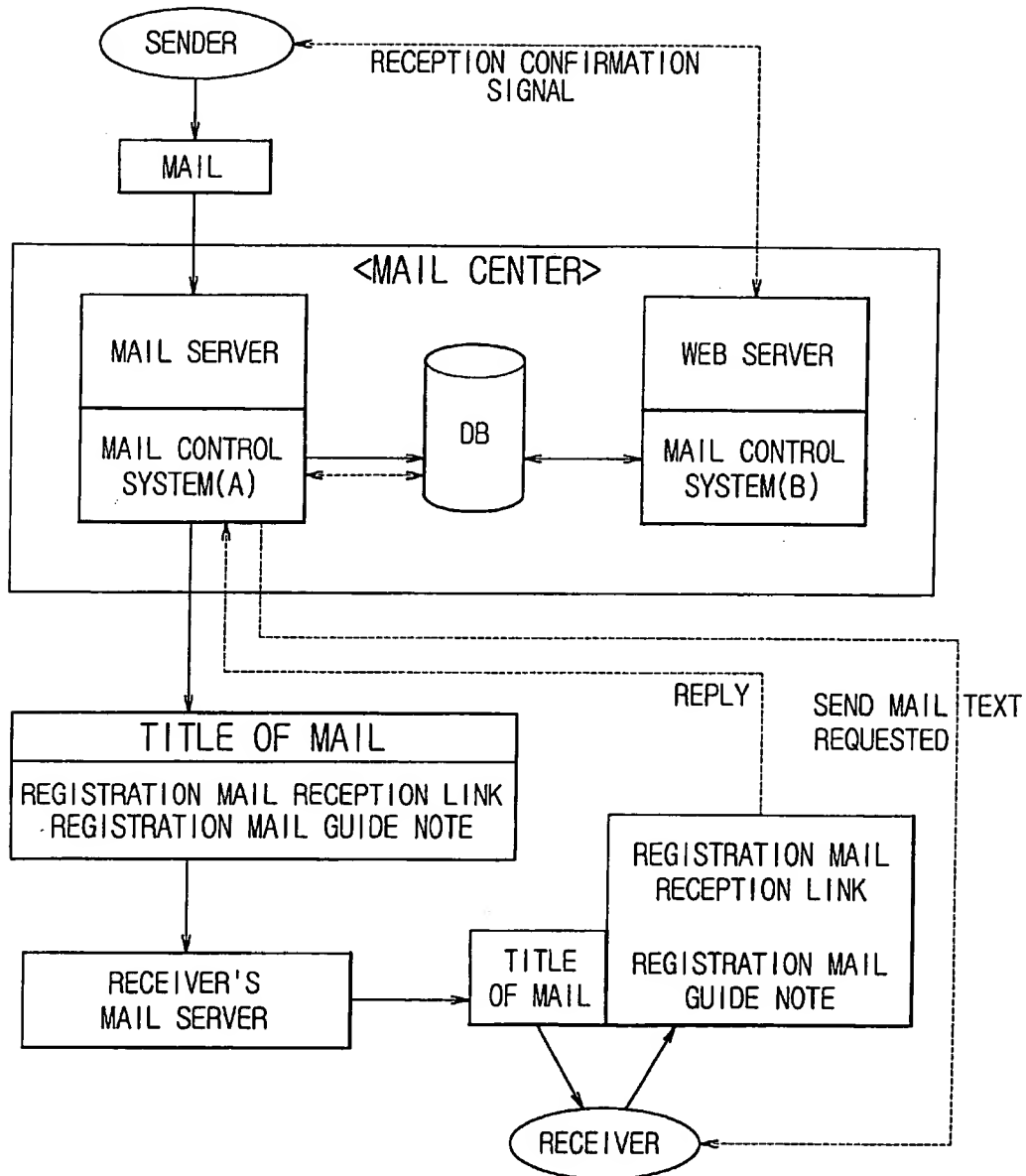


Fig.5



REGISTRATION MAIL SYSTEM WITH A SENT E-MAIL CHECK FUNCTION ON INTERNET AND METHOD FOR THE SAME

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a mail system and method for solving the problem that a sender cannot check whether or not a receiver received (read) a mail in an internet environment (FIG. 2) that is a switching system among mail servers independently operated.

2. Description of Related Art

Existing PC communication services (e.g., Chollian, Hitel, Nownuri, and Unitel in Korea) each provides a sent e-mail check function in exchanging mail between its own service users. This is possible because the service is a single mail system. However, the mail exchange between users of different services cannot be achieved. Namely, messages can be exchanged by e-mail only between users registered in the same service (FIG. 1).

On the other hand, users can freely exchange their message by e-mail regardless of services in which they registered according to the mail exchange system in the internet environment. Therefore, the existing PC communication services tend to provide an internet mail service together and the communication tends to be used based upon internet mail IDs (e-mail addresses). However, the existing internet mail service cannot provide a function allowing a sender to check whether or not a receiver read the mail sent by the sender. This is because internet mails are exchanged between independent mail servers. In this system, the sender cannot check the mail that the sender has sent to the receiver's mail server (FIG. 2).

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a registration mail system with a sent e-mail check function on internet and method for the same that substantially obviates one or more of the limitations and disadvantages of the related art.

An objective of the present invention is to provide a registration mail system with a sent e-mail check function, wherein a unique code is given to each mail sent by a sender and recorded in a database (DB), a common gate interface (CGI) executive program through which the unique code and confirmation information are sent to a source mail system if a receiver reads the mail is attached to the mail itself which is sent to the receiver's mail server, if the receiver reads the mail, the unique code and confirmation information that have been sent to the mail center by the CGI executive program are compared with database information and recorded in the database, and confirmation of reception by the receiver is notified to the sender.

Additional features and advantages of the invention will be set forth in the following description, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the invention will be realized and attained by the structure as illustrated in the written description and claims hereof, as well as the appended drawings.

To achieve these and other advantages, and in accordance with the purpose of the present invention as embodied and broadly described, the present invention employs a mail control system for assigning a unique code to a mail sent by a sender, recording the code in a database, and attaching a CGI executive program to the mail. The mail control system organically acts with a mail server and is in linkage with a database.

The present invention also employs another mail control system for comparing reception confirmation information from a receiver with database information, recording the confirmation information in the database, and sending an informing signal to the sender. This mail control system organically acts with a web server and is in linkage with the database.

When the receiver reads the mail in an off-line state, if a mail client application used by the receiver for reading the mail does not support a hypertext markup language (HTML), or if a text based emulator is used for reading the mail, the above system cannot be applied, so a registration mail system is developed as an extended type based upon the above system. In stead of using the program attached to the mail to process the reception confirmation information, the registration mail system stores the text of the mail therein and first sends only the information of a title of the mail, registration mail reception link, and registration mail guide note to the receiver. If the receiver requests the text of the mail, the registration mail system sends the text of the mail to the receiver and records the reception of the mail in the database.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE ATTACHED DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

In the drawings:

FIG. 1 is a block diagram showing a conventional mail system in PC communication;

FIG. 2 is a block diagram showing a conventional e-mail system in an internet environment;

FIG. 3 is a block diagram showing an overall structure of a mail system with a sent e-mail check function according to the present invention;

FIG. 4 is a block diagram showing an overall structure of an embodiment of a registration mail system with an extended sent e-mail check function according to the present invention; and

FIG. 5 is a block diagram showing an overall structure of another embodiment of a registration mail system with an extended sent e-mail check function according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

With reference to the accompanying drawings, the present invention will be described in detail.

FIG. 3 is a block diagram showing an overall structure of a mail system with a sent e-mail check function. Once a user composes a mail message and send it through this system, the mail is processed by a mail control system A which organically acts with a mail server. At this time, a unique code is assigned to the mail and the related information is recorded in a database. The mail control system A attaches the unique code and CGI executive program to the mail before sending it to the mail server of a receiver. If the

3

receiver reads the arrived mail, the CGI executive program is carried out so as to send information confirming the read of the message by the receiver and the unique code of the mail to a mail control system B in a mail center. The received mail code is compared with the mail codes previously recorded in the database to find the same mail code. Reception confirmation information is added to the corresponding mail record in the database. Thereafter, the mail control system B sends a reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. 3).

A registration mail system extended from the above system is similar to the above system in that a unique code is assigned to a mail sent by a sender. However, differently from the above system, the text of the mail is separately stored and a registration mail reception link and a registration mail guide note (indicates registration mail receive method for a user checking e-mail with an emulator based upon text) are attached to the mail in the mail center before sending the mail to the receiver's mail server. Once the receiver receives (reads) the mail, the text of the mail stored is requested through the registration mail reception link attached to the mail. The mail text is then received by the receiver through direct connection. At this time, the mail control system B compares the unique code of the mail with the mail codes in the database and adds reception confirmation information to the record of the corresponding mail in the database. Subsequently, the mail control system B sends the reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. 4).

However, if a mail client application used by the receiver for checking e-mail does not support HTML, or if the receiver checks the e-mail using the text based emulator, the above system cannot be applied. In this occasion, once the receiver just replies according to the content of the registration mail guide note, the mail control system A requests the text of the mail stored in the DB and sends it to the receiver. The mail control system A compares the unique code of the mail with the mail codes recorded in the DB and adds the reception confirmation information to the record of the corresponding mail. Thereafter, the mail control system B sends the reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. 5).

Consequently, the present invention makes it possible to use a sent mail check function on internet, thereby overcoming the defect of the internet e-mail that has been the main method for mail exchange.

As illustrated, the present invention embodies an internet mail system supporting a sent mail check function. This is sufficiently important to the part of e-mail as means of communication. For example, when the e-mail is used for business, there may be some cases the success of the business depends on whether or not the receiver reads within a certain time limit. There may be some cases that reception itself is refused or that a sender cannot check whether or not the receiver reads the mail by phone or other means. The sent mail check function is very important to the sender in these cases as well as daily mail exchange. In case a receiver uses a plurality of e-mail addresses, the present invention makes it possible for a sender to find and send e-mail to the receiver's e-mail address that is not used frequently. As illustrated, the sent mail check function is very useful. As internet e-mail becomes more important and necessary as means of communication, effect of the sent mail check function achieved by the present invention increases.

It will be apparent to those skilled in the art that various modifications and variations can be made in the registration

4

mail system with a sent e-mail check function on internet and method for the same of the present invention without deviating from the spirit or scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. An electronic mailing method on the Internet with a function of reception confirmation comprising:

(a) assigning a unique code to an e-mail of a sender and recording in a database the information on the unique code assigned to the e-mail;

(b) attaching to the e-mail, to which the unique code was assigned in the step of (a), a CGI (common gateway interface) executive program that automatically sends to the web server of the sender the unique code that was assigned in the step (a) when the receiver receives the e-mail;

(c) sending the unique code of the received e-mail to the web server of the sender by the automatic execution of the CGI executive program when the e-mail, to which the unique code was assigned in the step of (a) and to which the CGI executive program was attached in the step of (b), is received by the receiver; and

(d) comparing the unique code of e-mail that was sent in the step (c) and the unique code that was recorded in the step (a) and, if they are identical, sending reception confirmation information to the sender.

2. An electronic mailing method on the Internet with a function of receipt confirmation, comprising the steps of:

(a) assigning a unique code to an e-mail sent by a sender and storing the unique code in a database;

(b) attaching a CGI executive program to the e-mail containing the unique code of step (a) in order to transmit the unique code which is assigned to the e-mail in step (a), to an e-mail system of the sender upon a receiver's receipt of the e-mail;

(c) transmitting the unique code of the e-mail received by the receiver to the e-mail mail system of the sender by an automatic execution of the CGI executive program upon the receiver's receipt of the e-mail which contains the unique code and the CGI executive program of step (b); and

(d) delivering receipt confirmation information to the sender of the e-mail if the unique code of the e-mail transmitted in step (c) is identical to the information stored in the database.

3. An electronic mailing system on the Internet with a function of receipt confirmation, comprising:

a first mail control system having a mail processor part which assigns a unique code to e-mail sent by a sender, attaches a CGI executive program for e-mail transmitting the assigned unique code to the electronic mailing system upon a receiver's receipt of the e-mail, and transmits the e-mail to the receiver's mail server;

a database in which the unique code assigned by the mail processor part is recorded; and

a second mail control system having a receipt confirmation part which receives the unique code of the e-mail transmitted by automatic execution of the CGI executive program, compares the transmitted unique code with the unique code recorded in the database, and transmits receipt confirmation information to the sender if the two unique codes are identical.

* * * * *



US006618747B1

(12) **United States Patent**
Flynn et al.(10) Patent No.: **US 6,618,747 B1**
(45) Date of Patent: **Sep. 9, 2003**(54) **ELECTRONIC COMMUNICATION
DELIVERY CONFIRMATION AND
VERIFICATION SYSTEM**(76) Inventors: **Francis H. Flynn**, 14 Wave Crest Dr.,
Islip, NY (US) 11751; **Jeffrey Foran**,
1127 Commonwealth Ave., Apt. 1,
Allston, MA (US) 02134(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.(21) Appl. No.: **09/448,365**(22) Filed: **Nov. 23, 1999****Related U.S. Application Data**(60) Provisional application No. 60/109,934, filed on Nov. 25,
1998.(51) Int. Cl.⁷ **G06F 15/16**(52) U.S. Cl. **709/206; 709/203**(58) Field of Search **709/203, 206,
709/217; 345/744, 752; 379/93.24**(56) **References Cited****U.S. PATENT DOCUMENTS**

RE34,954 E	5/1995	Haber et al.	
5,426,594 A *	6/1995	Wright et al.	709/206
5,509,071 A	4/1996	Petrie, Jr. et al.	
5,675,733 A	10/1997	Williams	
5,748,738 A	5/1998	Bisbee et al.	
5,771,355 A *	6/1998	Kuzma	709/232
5,793,972 A *	8/1998	Shane	709/219
5,850,520 A	12/1998	Griebenow et al.	
5,903,723 A	5/1999	Beck et al.	
5,930,471 A *	7/1999	Milewski et al.	709/204
6,018,774 A	1/2000	Mayle et al.	
6,275,848 B1 *	8/2001	Arnold	709/206
6,332,164 B1 *	12/2001	Jain	709/235
6,385,655 B1 *	5/2002	Smith et al.	709/232
6,477,243 B1 *	11/2002	Choksi et al.	379/100.06

FOREIGN PATENT DOCUMENTS

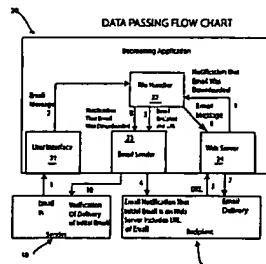
WO WO 02/25508 A2 * 3/2002

OTHER PUBLICATIONSGralla, P., *How the Intranets Work*, Ziff-Davis Press, pp. xi
& 122-125, 1996.*Stallings, W., *Data and Computer Communications*, Pren-
tice-Hall, pp. 728-730, 1997.*Lowe, D., *Client/Server Computing for Dummies*, IDG
Books Worldwide, pp. 125-128 and 136-137, 1995.*Gralla, P., *How the Internet Works*, Special Edition, Ziff-
Davis Press, pp. 76-86, 110-111 and 122-125.*Microsoft Press Computer Dictionary, 3rd ed., Microsoft
Press, pp. 34-35, 1997.*Klensin et al; Request for Comments: RFC 1869 (Nov.
1995) available at <http://www.gssnet.com/rfc/rfc1869.htm>,
pp. 1-11.Freed; Request for Comments: RFC 2034 (Oct. 1996) avail-
able at <http://www.gssnet.com/rfc/rfc2034.htm>, pp. 1-5.Mosher, Sue; *Microsoft Exchange User's Handbook*; Duke
Press (1997); pp. 220, 285, 288.Blue Mountain Arts. *Frequently Asked Questions*. [www.
bluemountain.com/help/FAQ2.html](http://www.bluemountain.com/help/FAQ2.html), pp. 5-6 & 11.

* cited by examiner

Primary Examiner—Andrew Caldwell(74) *Attorney, Agent, or Firm*—Collard & Roe PC(57) **ABSTRACT**

The present invention provides a system and a method for a user to verify receipt of an electronic communication such as an email message by an intended recipient. Instead of forwarding the email to the intended recipient(s), (e.g. as a normal SMTP server might,) the invention sends a notification message of a posted email to the intended recipient(s). The email and attachments are each saved at a unique call address on a server such as for example a web server. At least one unique address is provided for each of the intended recipients that points to the location of the contents of the original email. When attachments accompany the email, each attachment is also assigned an address that is unique for each intended recipient. The intended recipient is notified of the call addresses for collecting the email and attachments. When the recipient downloads or collects the email and attachments from their respective addresses, the invention detects information regarding the downloaded email and notifies the sender that the email was retrieved. This information may be stored in a back-end database for ease of access and management.

6 Claims, 2 Drawing Sheets

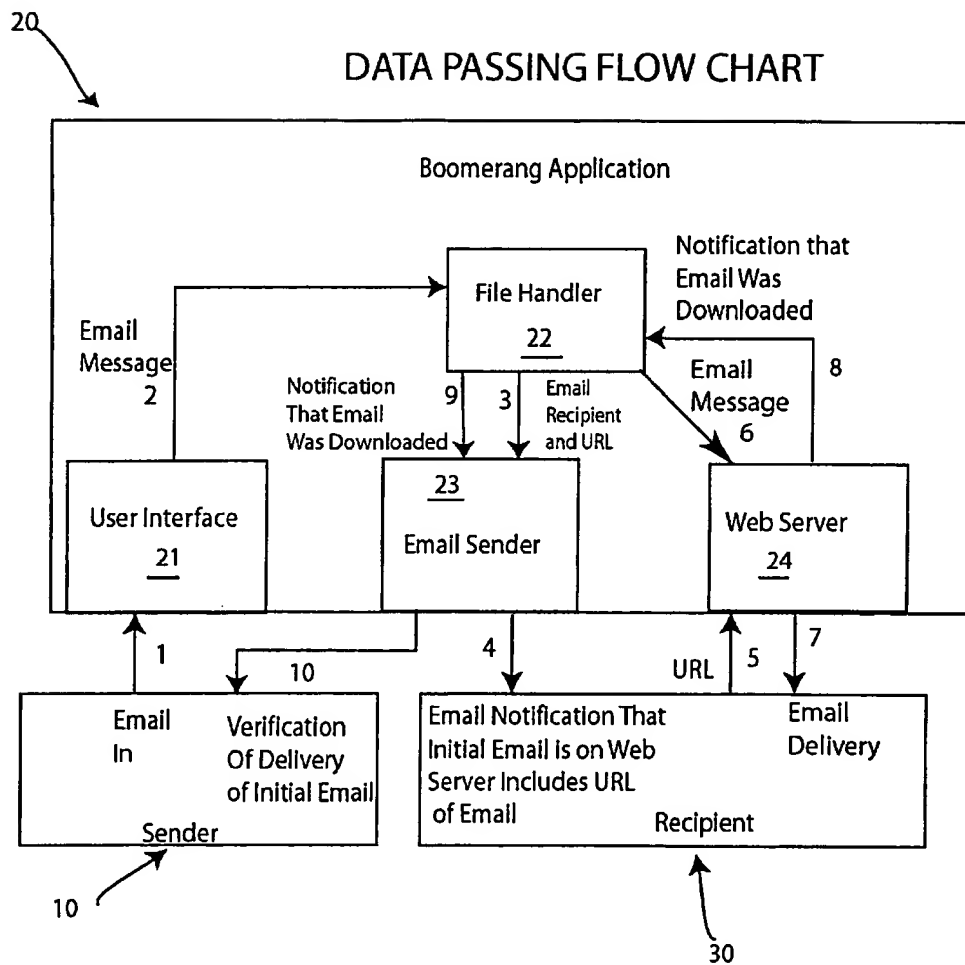
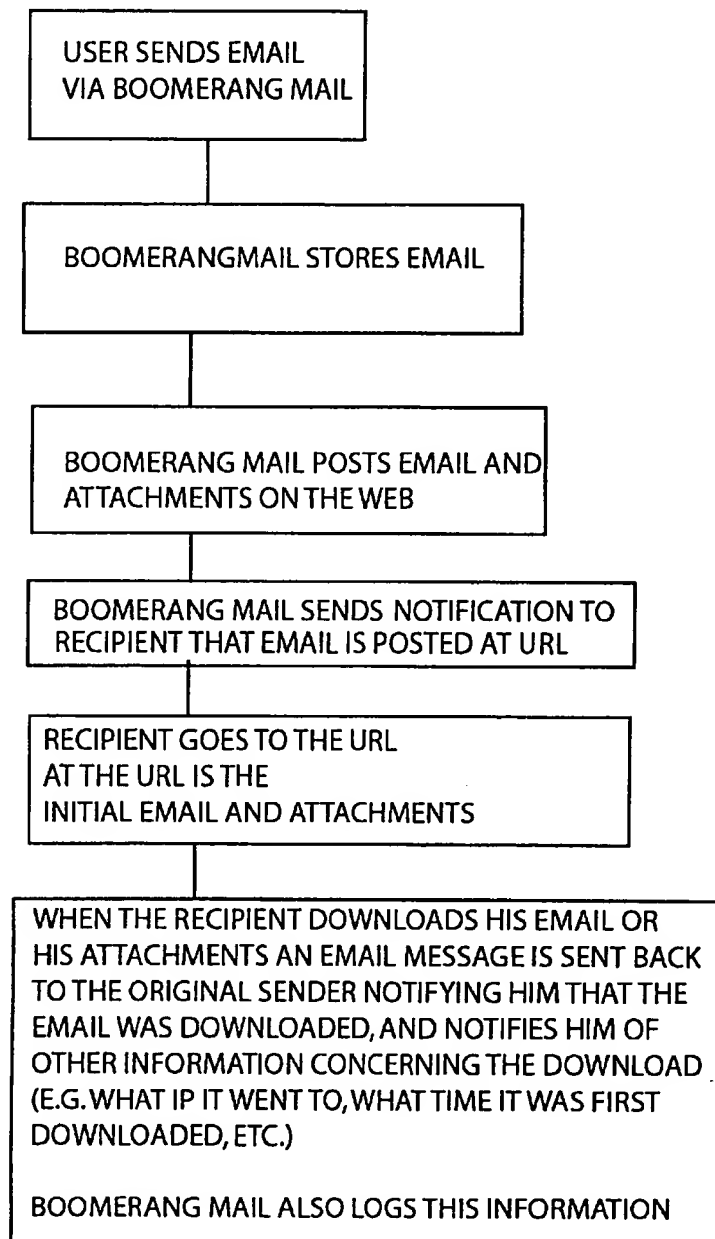


FIG. 2

SEQUENCE OF STEPS TAKEN DURING
BOOMERANG MAIL USE

ELECTRONIC COMMUNICATION DELIVERY CONFIRMATION AND VERIFICATION SYSTEM

This application claims the benefit of U.S. Provisional Patent Application 60/109,934 filed Nov. 25, 1998, entitled "An Electronic Communication Delivery Verification System", the content of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

This invention relates generally to electronic communications and, more particularly, to a method by which a sender of an electronic communication can validate receipt of an electronic communication by an intended receiver.

BACKGROUND OF INVENTION

Electronic communication, such as for example e-mail, is a form of written data, a data-string, that is transported electronically such as on the Internet. Specific protocols governing certain aspects of the way one machine electronically passes information in the form of data-strings to another machine have been established to facilitate communication between different brands of machines running different software. Various protocols have been developed to standardize the methods by which data are transported from one computer to another computer such as on Local Area Networks (LAN), Wide Area Networks (WAN), and the Internet. This standardization was developed to allow computers and computer programs from differing commercial sources to be as compatible as possible.

The Internet Protocol (IP) that directs or routes a data-string from one computer to another is what is called a best efforts protocol, a method that involves a series of computer instructions that attempts to deliver a data-string to its intended location, but that does not guarantee its delivery. This means that the data-string can get lost or damaged before reaching the intended recipient. The Transmission Control Protocol (TCP) works in conjunction with IP in an attempt to ensure that data-string is sent error-free, complete, and in the proper sequence. However, it does not insure correct delivery. The Simple Mail Transfer Protocol (SMTP) provides for standardized error messages to be issued when a fault occurs in transmission. Standardized status codes (such as described in Kleinsin, et al; Network Working Group Request for Comments: 1869; STD: 10; Obsoletes: 1651; Category: Standards Track; November, 1995) provide information for generating error messages that indicate whether or not a computer in the net or network of computers used to pass the data-string has been unable to do so. Such an Error message is exemplified by:

"---The following addresses had delivery problems ---
<nosuchuser@dbc.mtvview.ca.us>
(Mailbox "nosuchuser" does not exist)"

When delivery occurs a message such as "---Mail was successfully relayed to the following addresses---" may be provided. However, no information is provided by through the use of these protocols via the respective protocol server regarding whether the intended recipient has retrieved the email and/or the attachments.

Business people and others need to verify that an important transaction once sent has been received by the intended recipient. The main obstacle to widespread commercial use of electronic communications, such as for example email and email attachment, is the lack of the ability to verify that the email and/or attachment was received by the intended

recipient. Email must be sent on unsecured pathways, pathways where the email can be mis-directed, lost, and/or altered. It is highly desirable to the sender to be able to verify that the intended recipient has received an important email. It is also desirable to the sender to know that the intended information in electronic message was received as written or sent.

SUMMARY OF INVENTION

The instant invention comprises a software application for use with a computer that is part of or has access to an electronic network including at least one other computer and a method for use of the software application that provides a sender of an electronic communication such as an email, a receipt for verification of delivery of the electronic communication by a recipient. The sender may use a conventional email program or the instant invention to compose the email. The email ("electronic mail") may have graphics and/or attachments, each of which is termed a data-string herein. Unlike a conventional email program, each data-string is directed to a unique electronic address, such as for example an IP (Internet Protocol) address or hostname, on a computer that is independent of the recipient's computer. Only a notification that an email or an email plus an attachment is awaiting retrieval is sent to the recipient and appears at their computer. The notification provides the recipient with the unique electronic retrieval location(s), such as a unique IP address for an email message or two unique email addresses for an email accompanied by an attachment, located on a mail server to which the recipient can direct their computer using software to retrieve the data-string(s). Each recipient is provided with a unique address to retrieve their email even when the recipient is merely receiving a copy of an email that has been broadcast to a number of recipients. In one embodiment, a computer having access to the Internet is used as the mail server. In an alternate embodiment, the mail server is located on a LAN (local area network) such as for example for use for infra-office email within a business. Upon retrieval of the data-string, the sender is notified electronically via email and information regarding the retrieval transaction is stored in a back-end database.

For example, when the data-string is sent via the Internet, the user who is the sender composes an email message and attaches any text or images as required. Once the message is composed and sent, the instant invention parses that data-string while determining the appropriate recipients. The parsed data-string is placed on the World Wide Web (also termed the Web or the Internet or the Net) by waiting until at least one appropriate data-string transfer and retrieval means, such as for example a HyperText Transport Protocol (http) call provides an available address at a port of a computer the instant invention is monitoring. More addresses will be needed to match data-string to address when, for example, a single email data-string is being communicated to a number of different recipients. There is exactly one unique address that will access the data-string for each specific recipient targeted to receive the data-string unless the data-string has more than one component such as a plurality of attachments. Concurrent with posting the sender's data-string on a computer connected to a network of computers such as the Web, the instant invention sends out a notice via email that the recipient has a posted data-string or email awaiting retrieval. This message is simply a notice of the availability of the electronic communication that provides an electronic address such as a Uniform Resource Locator (URL) pointer to where the email is posted on the Web. One URL points to a single location that

is uniquely assigned for each component of the data-string for each recipient using the instant invention. Alternatively, the posted email may have a URL that allows it to call for its accompanying attachment i.e. the email and its accompanying documents may be electronically interlinked.

When the recipient of the email message links to a data-string via the URL pointer, the instant invention identifies the recipient by their unique IP address or hostname. As the recipient retrieves their posted email message and attachments, the instant invention notifies the sender that the posted electronic communication has been retrieved by a person at the IP address corresponding to that of the intended recipient. This notice includes the recipient's unique IP address or hostname and a time, date stamp indicative of when the posted electronic communication was retrieved. A copy of the posted electronic communication may also be included in the notice.

An embodiment of an inventive method for verifying receipt of an electronic communication at an intended electronic address is provided by the following example comprising the steps of:

1. Sending an electronic communication comprising a data-string.
2. Posting that data-string to a unique URL on a computer connected to the Web for each unique data-string.
3. Notifying the recipient at a recipient IP address via email that they have an electronic communication awaiting retrieval at a specified unique Web URL address.
4. Validating the retrieval of the sender's electronic communication by a recipient at an intended IP address by recognizing the recipient's IP address or hostname when they electronically request delivery of their electronic communication.
5. Notifying the sender when the IP address or hostname match the intended IP address or hostname that the electronic communication has been retrieved and optionally passing the validating information into a back-end database.

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

In one embodiment, the instant invention communicates (also termed "interfaces") with electronic communications program, such as for example email programs Eudora®, First Class Client®, and Hot Mail®. It can be used for electronic communication on the Internet or an Intranet, within a Local Area Network (LAN) or a Wide Area Network (WAN) environment. The invention provides a plurality of fields for data in the back-end database. Full search, browse, edit, and contact management functions are included in order to provide complete access to the stored data. Remote access functions may be configured. Thus, verification, authentication, and ease of data management are provided. Advantageously, the flow of electronic communications such as email can be controlled and documented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 provides a block diagram of the system and method by which an electronic communication in the form of data can be routed by a sender to a specific receiver and by which the sender can be notified of the receipt of the electronic communication by the specific receiver.

FIG. 2 provides a flow chart of the pathway and components used to transmit and verify an electronic communication.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The instant invention provides a system and method for confirmation of receipt of an electronic communication by an IP address or hostname accessible recipient ("the recipient"). The invention is a software application that allows the sender of an electronic communication to use the electronic communication program of their choice, such as for example an email program like Eudora®, to generate a specific data-string or message, send it to a specific recipient, and verify that the specific recipient received the data-string. Optionally, the application may provide a copy of the retrieved data-string so that the sender can determine if the data-string was received as sent, unaltered. Transmission of electronic information involves passing data in the form of a data-string from one computer to another through the use of computer programs that convert user instructions into instructions that a computer can understand. The data-string is then passed through electronic means, such as for example by telephone wires or cables, from one computer to another computer. These computers form a network of computers that is variously referenced to as a "Net" or "Web".

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This

5

interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

Referring now to FIG. 1 which illustrates a first embodiment of the instant invention, when an electronic communication sender is distanced from a recipient and the Internet is used to send the electronic communication, a sender illustrated by box "Sender" 10 enters information, such as for example an email message and an attachment to that email message, into a computer via the desired electronic communications program that has been loaded on that sender's machine. A message data-string is generated. This message data-string is then processed by the instant invention which has been loaded on the sender's machine as follows. The message data-string is parsed into an html-readable file and electronically sent via a user interface 21 to a file handler 22 where the message data-string is stored at a unique http call address assigned to each of the intended recipients. Assignment of the unique http call address(es) is determined by the instant invention which monitors a port for incoming TCP connections. If the electronic communication was an email that included an attachment, then a unique address is assigned to each of the parsed original email message and original attachment html-readable files. Concurrently upon receiving a file for storage, the file handler also generates a unique data-string for each stored file that is a notification message that is delivered to each unique recipient. This notification data-string informs each recipient that one unique message data-string has been stored for them at the indicated unique http call address. This notification data-string is sent via a Web Server 24 to the intended unique recipient, represented by box "recipient" 30.

The notification data-string may have additional information added to it prior to its delivery to the recipient. For example, the electronic communication sender's name and/or email address may be added. Or, an advertisement may be added to the notification message data-string.

The notification message data-string is then sent to the recipient's Post Office Protocol (POP) server and is read by the recipient at the notified IP address or hostname address indicated by the notification message when they open their email application. If the recipient wishes to read the posted electronic communication, the recipient enters the unique http call address that has been sent in the notification message data-string and retrieves the unique message data-string from the Web Server 24, if the recipient has entered the correct http call address. Both an email and its associated attachment(s) can be provided with unique call addresses or the email and its attachment(s) can be linked so that the entire communication is available using one call address. In a first embodiment for each stored message data-string retrieved, be it email or attachment, the Web server sends a notification of receipt message that informs the sender that the message data-string was retrieved by the recipient at the address receiving the notification of available email and http call address. This notification of receipt message is electronically transmitted to the sender at approximately the same time that the recipient is sent (retrieves) the stored message data-string. The notification of receipt message is

6

sent via the file handler and the email sender to the IP or hostname address of the sender ("original sender") and includes information concerning the downloading of the message data-string by the recipient, such as for example, the time it was first downloaded (time and date stamp), the address to which it was sent at downloading, and other relevant information. A compressed copy of the message received by the recipient may also be provided to the sender.

If the original electronic communication comprises an email and an attachment, then in one embodiment, the recipient is notified that an electronic communication is located at http call address 1 (the email) and at http call address 2 (the attachment). The recipient retrieves the electronic communications at each address and notification of each separate retrieval is provided to the sender as described above. Alternatively, the notification message may contain a link to the address for the email and to the address for the attachment. Notification of receipt may then be sent as each data-string is retrieved or notification of receipt may be sent only once when all associated electronic communications have been retrieved.

FIG. 2 provides an embodiment of a method of confirming that an electronic communication was received by a recipient. This embodiment exemplifies electronic communication verification when using the Internet to transport the electronic communication. Referring now to FIG. 2, a flow-chart of the steps used to provide verification to a sender that receipt of a electronic communication by a recipient has occurred is provided. The sender installs the software, the inventive computer program for generating electronic mail receipts, on their computer and electronically moves through a set-up interface. The sender generates an electronic communication such as an email. The sender enters the email address of the intended recipient or recipients thus providing an addressed packet of information or a message data-string which includes the address of the intended recipient that is unique for each intended recipient. The message data-string is converted to html-readable language and passed to a file handler via a user interface. The message data-string is stored while the instant invention locates one unoccupied call address, such as for example an http call address, if the message data-string is going to only one recipient. Otherwise, the instant invention recognizes that a plurality of unique call address are required and establishes one unique call address for storage of each copy of the email sent to the plurality of intended recipients. In the simplest case where there is one recipient, the message data-string is then posted to this unique unoccupied call address which is on a Web server. Concurrently, a notice that the recipient has email from the sender on the Web server at the call address at which the message data-string is located is sent to the recipient's Post Office Protocol (POP) server, notifying the recipient that they have an electronic communication. The recipient requests the message data-string located at the provided unique call address and it is sent to the recipient, who downloads it, opening it. Upon downloading of the message data-string, the instant invention generates a notice of receipt that is forwarded to the original sender. The notice of receipt forwarded to the sender at the sender's POP server includes information concerning the collection of the email by the recipient such as for example the address to which the email was downloaded, the time it was downloaded, and optionally, a compressed copy of the original message. When the sender enters their POP server, they receive the notification of receipt by the recipient.

When attachments accompany an email, each of the attachments and the email itself is provided with a unique

call address. Each is collected separately by the intended recipient. The intended recipient may be notified of each separately or the intended recipient may be directed to the email call address which then provides the recipient with the unique call addresses of each of the attachments.

Notification of receipt of the email and attachments can be achieved in a variety of ways and may vary depending upon the number of recipients and the number of attachments sent. Notification can be sent as each unique recipient accesses each unique call address. Or, notification may be sent to the sender when the recipient has collected the email and all of its associated attachments. Or, where a plurality of recipients have been sent the same email, the sender may be notified only after all the recipients have retrieved their copies of the email. Preferably, in the notification of receipt, a copy of the electronic message as received by the recipient is included. This message may then be compared with the message sent to verify that the message was not garbled during transmission. Other options will be apparent to those skilled in the art.

The instant invention also may be inactivated without having to remove the software application off the computer hard disc. The instant software application is provided with the following switches: Override, Always On, and Switch. Override allows the user to substantially turn off the software application thus deactivating notification of receipt. "Always On" allows the user to send electronic communication which provides notification of receipt whenever the electronic communication is accessed. Switch provides a subroutine that reads the electronic communication before it is sent by the sender to determine if a receipt is being requested.

Modifications and variations can be made to the disclosed embodiments without departing from the subject and spirit of the invention as defined in the following claims. Such modifications and variations, as included within the scope of these claims, are meant to be considered part of the invention as described.

What is claimed is:

1. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

- a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;
- b) posting said data-string having said electronic address to a unique call address;
- c) providing the intended recipient with said unique call address at said electronic address;
- d) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;
- e) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string;
- f) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

2. The method as in claim 1, further comprising the step of posting said data in a back end database.

3. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

- a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;
 - b) sending an attachment to said electronic communication to an additional electronic address for the intended recipient;
 - c) posting said data-string having said electronic address to a unique call address;
 - d) posting said attachment having said additional electronic address to an additional unique call address;
 - e) providing the intended recipient with said unique call address at said electronic address;
 - f) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;
 - g) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string; and
 - h) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.
4. The method as in claim 3, further comprising the step of posting said data in a back end database.

5. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

- a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;
- b) means for posting said data-string having said electronic address to a unique call address;
- c) means for providing the intended recipient with said unique call address at said electronic address;
- d) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;
- e) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said datastring; and
- f) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

6. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

- a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;
- b) means for sending an attachment to said electronic communication to an additional electronic address for the intended recipient;
- c) means for posting said data-string having said electronic address to a unique call address;
- d) means for posting said attachment having said additional electronic address to an additional unique call address;

9

- e) means for providing the intended recipient with said unique call address at said electronic address;
- f) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;
- g) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data

10

- string when said electronic address in said request matches said electronic address in said datastring; and
- h) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

* * * * *



US005748738A

United States Patent [19]

Bisbee et al.

[11] Patent Number: **5,748,738**[45] Date of Patent: **May 5, 1998**

[54] **SYSTEM AND METHOD FOR ELECTRONIC TRANSMISSION, STORAGE AND RETRIEVAL OF AUTHENTICATED DOCUMENTS**

5,323,146 6/1994 Glaschick .
5,339,361 8/1994 Schwalm et al .
5,363,448 11/1994 Koopman, Jr. et al .

(List continued on next page.)

[75] Inventors: **Stephen F. Bisbee**, Gibson Island; **Jack J. Moskowitz**, Ellicott City; **Edward R. Sheehan**, Sykesville; **Douglas H. Trotter**; **Michael W. White**, both of Baltimore, all of Md.

OTHER PUBLICATIONS

CCITT Draft Recommendation X.411, Ver. 4e. §§ 8.3.1.1.2.2 and 8.3.1.1.2.3 (Jun. 1987).

Request for Comments 1114, "Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Management", IAB Privacy Task Force (Aug. 1989).

G.F. Hice et al., *DMS Prologue to the Government E-Mail Revolution*, J.G. Van Dyke & Associates, Inc., chapt. 3 (1995).

(List continued on next page.)

[73] Assignee: **Document Authentication Systems, Inc.**, Dallas, Tex.

[21] Appl. No.: **528,841**

[22] Filed: **Sep. 15, 1995**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 373,944, Jan. 17, 1995, Pat. No. 5,615,268.

[51] Int. Cl.⁶ **H04L 9/00**

[52] U.S. Cl. **380/25; 380/30**

[58] Field of Search **380/25, 30**

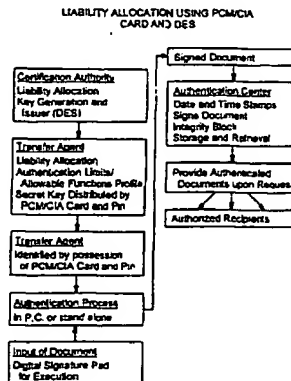
References Cited**U.S. PATENT DOCUMENTS**

Re. 34,954	5/1995	Haber et al. .	
4,200,770	4/1980	Hellman et al. .	
4,405,829	9/1983	Rivest et al. .	
4,625,076	11/1986	Okamoto et al. .	
4,853,961	8/1989	Pastor .	
4,893,338	1/1990	Pastor .	
4,981,370	1/1991	Dziewit et al. .	
4,995,082	2/1991	Schnorr .	
5,005,200	4/1991	Fischer	380/30
5,136,646	8/1992	Haber et al. .	
5,136,647	8/1992	Haber et al. .	
5,163,091	11/1992	Graziano et al. .	
5,164,988	11/1992	Matyas et al. .	380/25
5,191,613	3/1993	Graziano et al. .	
5,214,703	5/1993	Massey et al. .	
5,231,668	7/1993	Kravitz	380/30
5,276,737	1/1994	Micali .	
5,315,658	5/1994	Micali .	

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Burns, Doane, Swecker & Mathis, LLP

[57] ABSTRACT

Methods and apparatus are provided that implement digital signing and/or encryption for the electronic transmission, storage, and retrieval of authenticated documents and that enable the establishment of the identity of the originator of an electronic document and of the integrity of the information contained in such a document. Together these provide irrevocable proof of authenticity of the document. The methods and apparatus make it possible to provide "paperless" commercial transactions, such as real-estate transactions and the financial transactions secured by real estate. A Certification Authority provides tools for initializing and managing the cryptographic material required to sign and seal electronic documents. An Authentication Center provides "third party" verification that a document is executed and transmitted by the document's originator. The methods and apparatus eliminate the need for "hard copies" of original documents as well as hard-copy storage. Retrieval of an authenticated document from the Authentication Center may be done by any number of authorized parties at any time by on-line capability.

16 Claims, 10 Drawing Sheets

U.S. PATENT DOCUMENTS

5,371,794	12/1994	Diffie et al.	380/30
5,373,561	12/1994	Haber et al.	380/25
5,377,270	12/1994	Koopman, Jr. et al. .	
5,390,247	2/1995	Fischer	380/30
5,524,073	6/1996	Stambler .	
5,534,855	7/1996	Shockley et al.	380/25
5,555,307	9/1996	LeCorre et al. .	

OTHER PUBLICATIONS

D. Chaum, "Achieving Electronic Privacy", *Scientific American*, vol. 247, No. 8, pp. 96-101 (Aug. 1992).

W. Diffie et al., "Privacy and Authentication: An Introduction to Cryptography", *Proc. IEEE* vol. 67, pp. 397-427 (Mar. 1979).

W. Diffie, "The First Ten Years of Public-Key Cryptography", *Proceedings of the IEEE*, vol. 76, pp. 560-577 (May 1988).

M.E. Hellman, "The Mathematics of Public-Key Cryptography", *Scientific American*, vol. 234, No. 8, pp. 146-152, 154-157 (Aug. 1979).

C.R. Merrill, "Cryptography for Commerce—Beyond Clipper", *The Data Law Report*, vol. 2, No. 2, pp. 1, 4-11 (Sep. 1994).

L. Nadile, "Service Notarizes Electronic Documents", *PC Week*, pp. 29, 36 (Jan. 16, 1995).

R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126 (Feb. 1978).

C.E. Shannon, "Communication Theory of Secrecy Systems", *Bell Sys. Tech. J.* vol. 28, pp. 656-715 (Oct. 1949).

FIG. 1

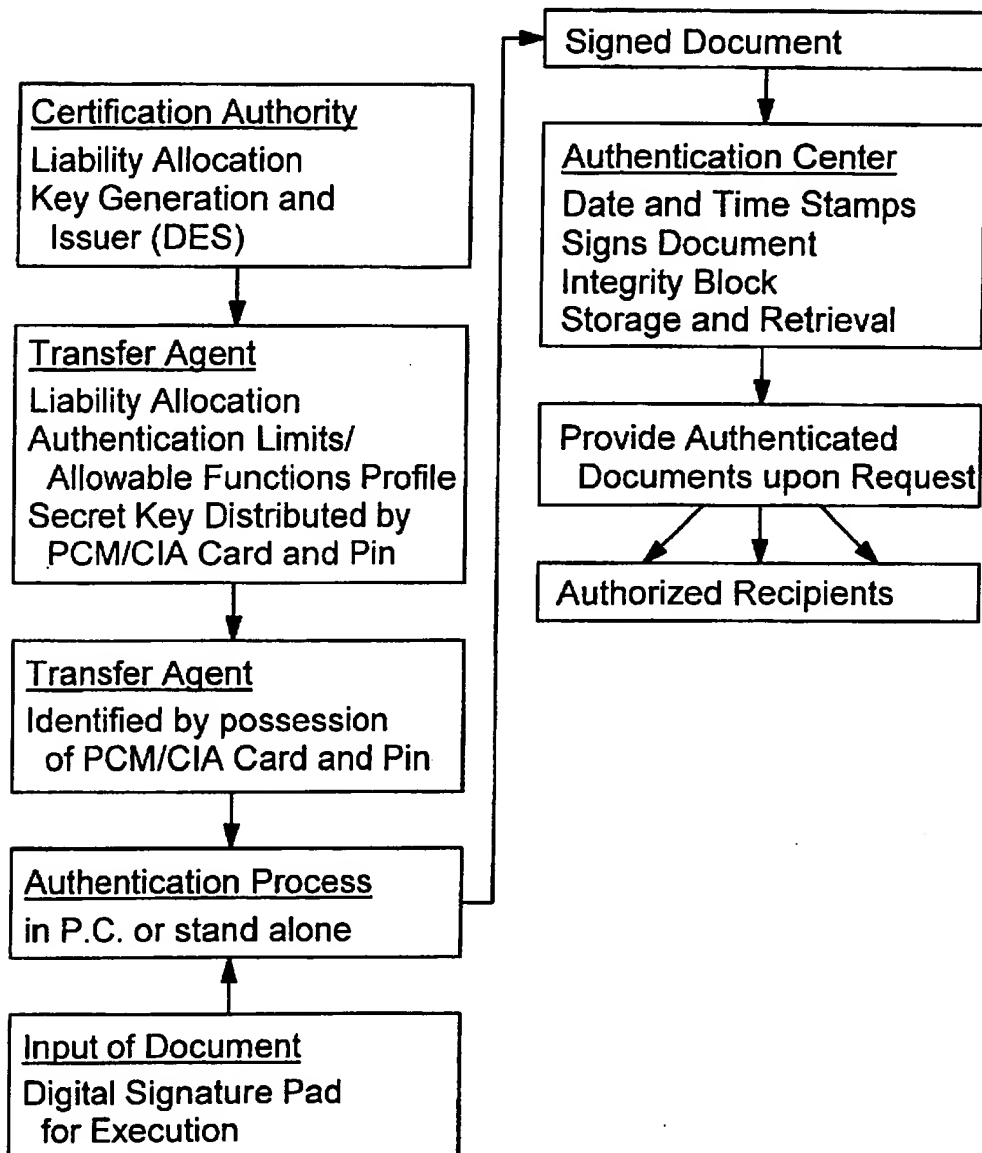
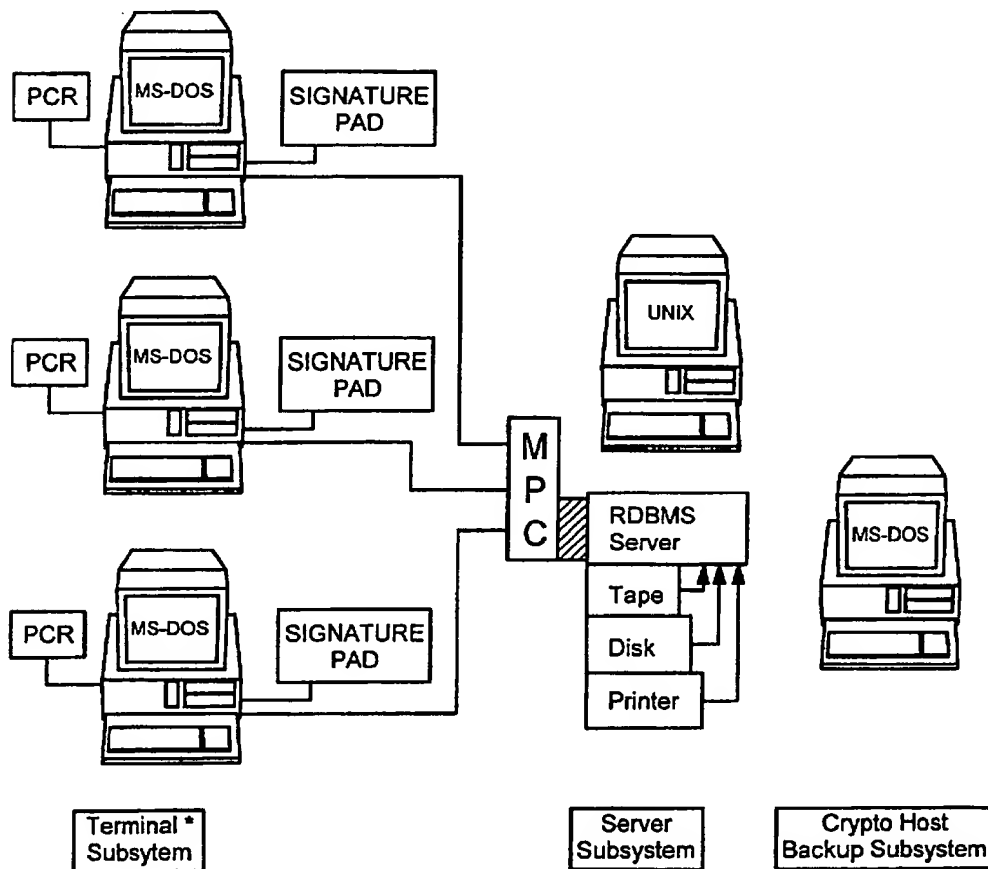
LIABILITY ALLOCATION USING PCM/CIA
CARD AND DES

FIG. 2

PCCard	Terminal Software	DAS Services
<i>Tamperproof cryptography</i> Provides cryptographic processing for: PIN - Card activation & exposure of secret cryptographic materials Key Exchange Key Set Management of encryption, hash, and signature keys Stores: Card Characterization Information Certificates & Keys Software macros Attribute tables	Card Resource Manager Participates in Card authentication & activation Format data & perform I/O operations with Card Requests Card services	PIN validation Compute integrity value Sign Authenticate Signature Validate Integrity Time-Stamp Encrypt/ decrypt Manage keys Store Audit Trail & Liability Allocation

FIG. 3

DAS ARCHITECTURE

TRANSFER AGENTSAUTHENTICATION CENTER

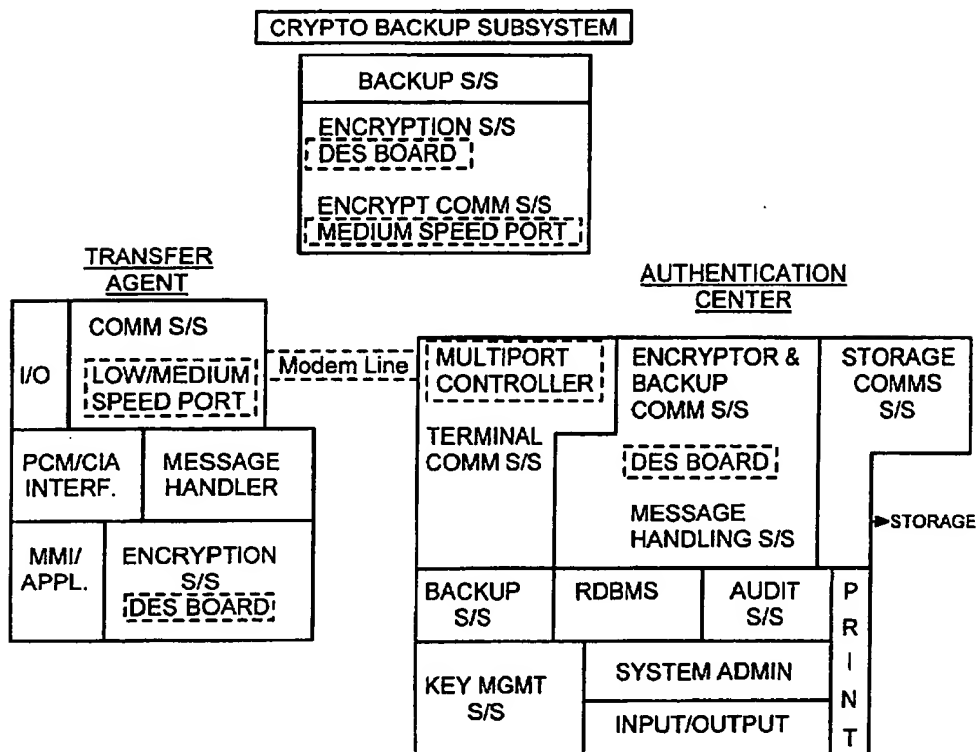
MPC - Multiport Controller

PCR - PCM/CIA Card Reader

* - 486/50 Laptop Computers
may be utilized

FIG. 4

DAS FUNCTIONAL INTERRELATIONSHIP

TERMINAL SUBSYSTEM

Terminal: 486/50 PC
MS/DOS
Windows

Running Agent Application
with transparent secure
communications

SERVER SUBSYSTEM

Server: 486/50 System Pro
UNIX

Built Around Powerful
multiuser RDBMS,
supporting multiple
terminal communications
with complete audit and
administration

Crypto Host: 486/50 PC
MS/DOS
Provides Encryption

FIG. 5

DAS CONTROL FUNCTIONS

CONTROL FUNCTIONS			
Confidentiality	Integrity	Non-repudiation (Signature) User	Authentication System Management Limits on User
Public key encryption of PIN and Keying Material	Digital Signature provides integrity protection.	Digital sign. of user/ customer "signs" the transactions in a manner that cannot be repudiated.	Limits for user profile stored on PCM/ CIA card
DES encryption of transactions.			PIN and PCM/ CIA card authentication to terminal and DAS system

FIG. 6a

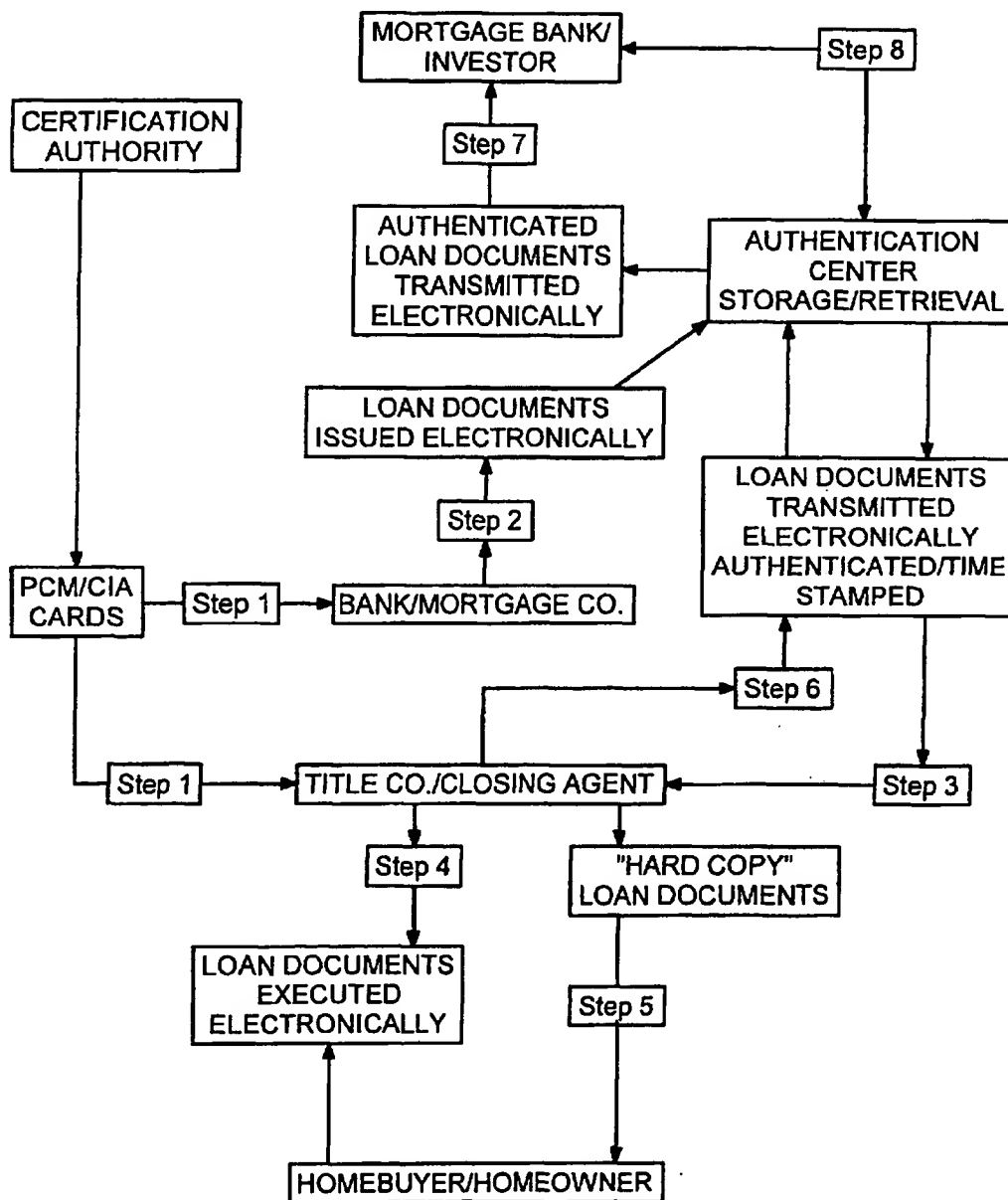
DOCUMENT AUTHENTICATION SYSTEM LOAN TRANSACTION

FIG. 6b

DOCUMENT AUTHENTICATION SYSTEM LOAN TRANSACTION

Chart Steps

- Step 1.** Complete Certification Authority code generation and card issuing to parties transferring the documents establishing legal evidence trail. Equip parties to transmit and receive documents
- Step 2.** Bank/ Mortgage Co. loads and electronically transmits documents to Authentication Center which forwards to Title Co./Closing Agent
- Step 3.** Authentication Center transmits documents to Title Co./Closing Agent
- Step 4.** Title Co./Closing Agent has documents executed by digital signature by Homebuyer/Homeowner
- Step 5.** Title Co./Closing Agent provides Homeowner/Homebuyer with "Hard Copy" of signed documents
- Step 6.** Title Co./Closing Agent transmits documents to Authentication Center which dates and time stamps the executed documents and forwards documents to Bank/Mortgage Co.
 - Whenever Bank/Mortgage Co. needs authentic documents, can retrieve on-line from Authentication Center storage
- Step 7.** Bank/Mortgage Co. directs authentic documents to be transferred by Authentication Authority to secondary market investor
- Step 8.** Whenever investor needs authentic documents, can retrieve on-line from Authentication Center

FIG. 7

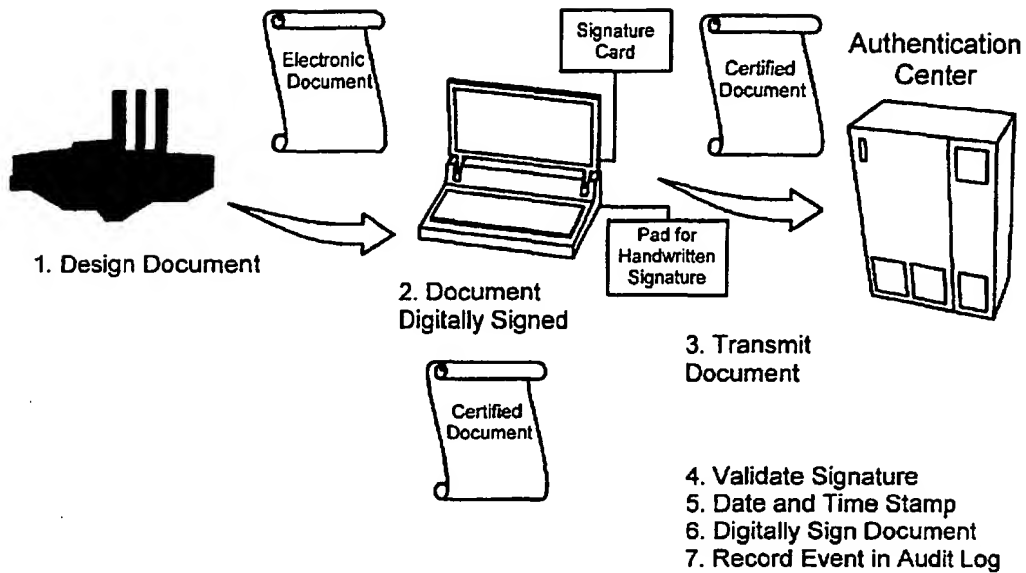


FIG. 8

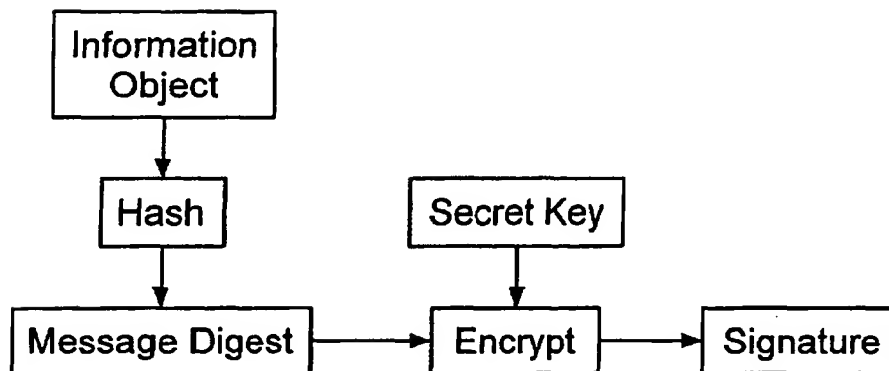


FIG. 9

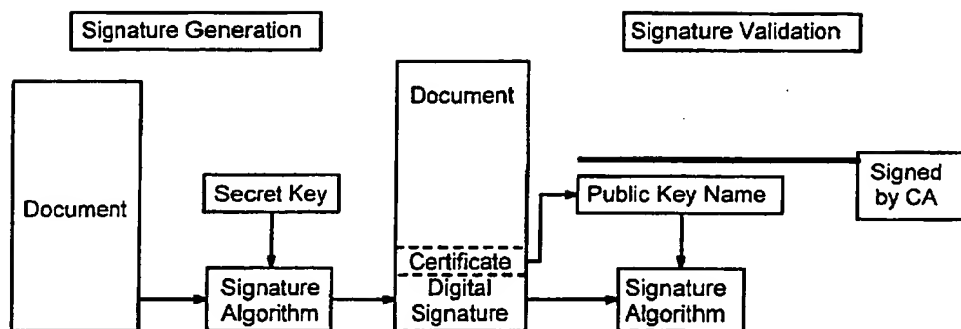


FIG. 10

CARICATURE OF X.509 CERTIFICATE
USER OR CERTIFICATION AUTHORITY

<u>IDENTITY</u>	<u>ATTRIBUTES</u>	<u>PUBLIC KEY</u>	<u>SIGNATURE VALUE</u>
Name/Organization	Various Privileges	Decrypt Info	Digitally Signed Message Digest of Certificate

FIG. 11

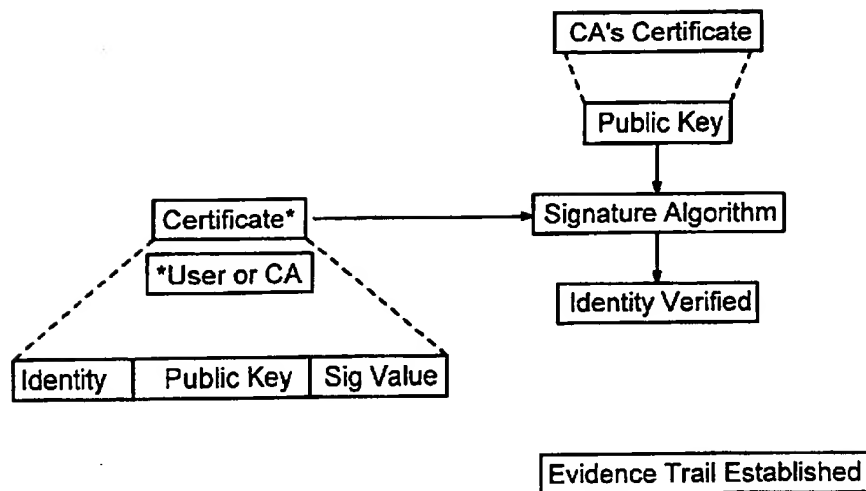
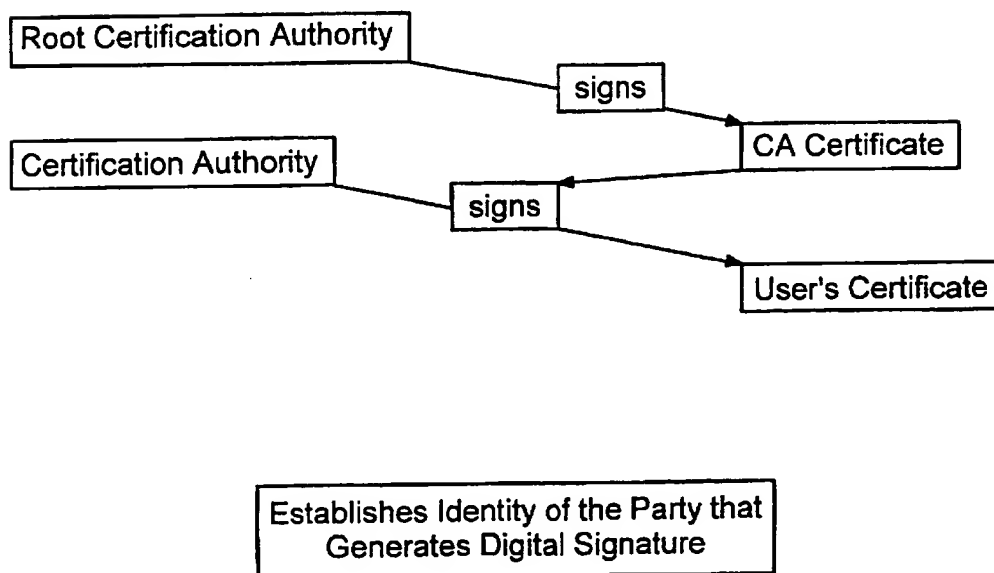


FIG. 12



SYSTEM AND METHOD FOR ELECTRONIC TRANSMISSION, STORAGE AND RETRIEVAL OF AUTHENTICATED DOCUMENTS

This application is a continuation-in-part of U.S. patent application Ser. No. 08/373,944 filed Jan. 17, 1995, now U.S. Pat. No. 5,615,268 by Stephen F. Bisbee.

BACKGROUND

Applicant's invention relates to systems and methods for providing a verifiable chain of evidence and security for the transfer and retrieval of documents in digital formats.

Paper documents are the traditional evidence of the communications and agreements between parties in commercial and other transactions. Financial and real-estate transactions are protected by paper-based controls. Signatures and safety paper (such as pre-printed checks) facilitate detection of unauthorized alterations of the information of commercial transactions. Important documents may also be provided with "third man" controls, by the witnessing of signatures and by the seal and acknowledgement of a Notary Public.

The methods of commerce, however, have changed dramatically and continue to evolve. This is most evident in the replacement of paper-based communications with electronic communications. The "due care" controls used with paper-based communications do not exist in routine electronic transactions. Standard electronic communication over open systems does not have the same ability to provide authentication, privacy, and integrity of the communicated information. By "authentication" is meant verification of the identity of the signatory of a document; by "privacy" is meant protection of the information in a document from unauthorized disclosure; and by "integrity" is meant the ability to detect any alteration of the contents of a document.

When communication is by electronically reproduced messages such as e-mail, facsimile machine, imaging, electronic data interchange or electronic fund transfer, there no longer exists a signature or seal to authenticate the identity of the transferor. The traditional legally accepted methods of verifying the identity of a document's originator, such as physical presence or appearance, an ink signature, personal witness or Notary Public acknowledgement, are not possible.

The continued evolution of computer and telecommunication technology has regrettably been accompanied by the invention of more sophisticated ways to intercept and alter information electronically transmitted, including the widespread phenomenon of remote intrusion of computer systems through telecommunication links.

Some approaches to providing secure electronic commerce technology by applying cryptography give the user a verification mechanism for the authenticity or privacy of the transmission that is controlled by the user and does not include the element of non-repudiation. In some cases the use of encryption for privacy could aid in the detection of document alterations, advancing the goal of integrity. This is not generally the case, however, and additional mechanisms may be required for providing integrity. At present, no distributed electronic document authentication system exists that can provide authentication, as with written or printed instruments, in a manner that cannot be repudiated. No commercial system provides electronic document verification based on a digital signature that cannot be repudiated, although some attempts have been described. See, e.g., D. Chaum, "Achieving Electronic Privacy", *Scientific*

American, vol. 247, no. 8, pp. 96-101 (Aug. 1992); C. R. Merrill, "Cryptography for Commerce - Beyond Clipper", *The Data Law Report*, vol. 2, no. 2, pp. 1, 4-11 (Sep. 1994). Since DES, no governmental organization or other standards-setting body has been willing or able to set standards (i.e., as to cryptographic strength, process, etc.) acceptable for general commercial use. The techniques described in this application are synergistic and of sufficient assurance to be on par with the security needed to support a typical business transaction.

Applicant's document authentication system (DAS) provides the needed security and protection of electronic transmissions, such as electronic documents. Most important to commercial and financial institutions, Applicant's DAS assumes the risk and responsibility of a document's authenticity. Applicant's DAS utilizes an asymmetric cryptosystem, known as a public-key system, to help ensure that the party originating a document is electronically identifiable as such when a DAS digital signature is applied.

Various aspects of public-key cryptographic (PKC) systems are described in the literature, including R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* Vol. 21, pp. 120-126 (Feb. 1978); M. E. Hellman, "The Mathematics of Public-Key Cryptography", *Scientific American*, vol. 234, no. 8, pp. 146-152, 154-157 (Aug. 1979); and W. Diffie, "The First Ten Years of Public-Key Cryptography", *Proceedings of the IEEE*, vol. 76, pp. 560-577 (May 1988). Popular PKC systems make use of the fact that finding large prime numbers is computationally easy but factoring the products of two large prime numbers is computationally difficult. A PKC system is an asymmetric encryption system, meaning that it employs two keys, one for encryption and one for decryption. Asymmetric systems adhere to the principle that knowledge of one key (the public key) does not permit derivation of the second key (the private key). Thus, PKC permits the user's public key to be posted (e.g., in a directory or on a bulletin board), without compromising his/her private key. This public key concept simplifies the key distribution process. Example PKC algorithms are the digital signature algorithm and secure hash algorithm (DSA/SHA) and RSA/MDS.

Besides the PKC method, another encryption method is the symmetric algorithm. An example of this is the Data Encryption Standard (DES), which is described in *Data Encryption Standard*, Federal Information Processing Standards Publication 46 (1977) ("FIPS PUB 46", republished as FIPS PUB 46-1 (1988) and *DES Modes of Operation*, FIPS PUB 81 (1980) that are available from the U.S. Department of Commerce. In general, a symmetric cryptographic system is a set of instructions, implemented in either hardware, software or both that can convert plaintext (the unencrypted information) to ciphertext, or vice versa, in a variety of ways, using a specific key that is known to the users but is kept secret from others.

For either a symmetric or PKC system, the security of a message is dependent to a great extent on the length of the key, as described in C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell Sys. Tech. J.* vol. 28, pp. 656-715 (Oct. 1949).

SUMMARY

These and other objects and advantages are provided by the DAS which comprises the means to identify the originator of the electronic document, to provide irrevocable proof of the integrity of an electronic document and the

means to prevent the originator of the document from denying the document's originator, i.e., non-repudiation.

In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes.

The signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest.

The method may further comprise the step of applying a date stamp and a time stamp to the electronic document. The date and time stamps may be applied either before or after validation of the digital signature and electronic document using the certificate. Also, the method may further comprise the step of signing the electronic document with a second digital signature.

In another aspect of the invention, an apparatus for authenticating an electronic document comprises means for signing the electronic document with a digital signature of a Transfer Agent; means for appending a certificate to the electronic document; and means for validating the digital signature and certificate. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes.

The signing means may comprise means for applying a hash function to the electronic document to determine a message digest and means for using the message digest with the Transfer Agent's secret cryptographic key to determine the digital signature. The validating means may then comprise means for decrypting the message digest with a public cryptographic key of the Transfer Agent, means for applying the hash function to the electronic document to determine a second message digest, and means for comparing the decrypted message digest to the second message digest.

The apparatus may further comprise means for applying a date stamp and a time stamp to the electronic document. The date and time stamps may be applied either before or after the digital signature and electronic document have been validated using the certificate. Also, the apparatus may further comprise means for signing the electronic document with a second digital signature.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of Applicant's invention will become apparent by reading this description in conjunction with the drawings in which:

FIG. 1 is a block diagram of the liability allocation for authentication in the DAS;

FIG. 2 summarizes the functions of the DAS relating to document transmission authorization and protection;

FIG. 3 is a simple diagram of the DAS architecture;

FIG. 4 is a block diagram of the functional interrelationship between a Transfer Agent and an Authentication Center;

FIG. 5 is a block diagram of DAS control functions;

FIGS. 6a, 6b are diagrams illustrating application of the DAS in the mortgage finance industry with a title company/closing agent for a loan as a Transfer Agent;

FIG. 7 illustrates the document certification process more generally;

FIG. 8 illustrates generation of a digital signature;

FIG. 9 illustrates digitally signing a document and validation of the digital signature;

FIG. 10 illustrates the format of a certificate employed by a user or the Certification Authority;

FIG. 11 illustrates validation of certificates; and

FIG. 12 illustrates generation of certificates.

DETAILED DESCRIPTION

Applicant's invention can be implemented utilizing commercially available computer systems and technology to create an integrated closed system for authentication of electronic documents.

Referring to FIG. 1, which is a block diagram of the liability allocation for authentication in Applicant's DAS, the DAS uses a Certification Authority framework by which public/private keys, that are utilized to encrypt/decrypt and/or digitally sign a document, are delivered to a document's originator by an established, auditable means. Certificates and certification frameworks are described in the above-cited publication by C. R. Merrill and in ITU-T Recommendation X.509 (1993)/ISO/IEC 9594-8: 1995 Information Technology - Open Systems Interconnection - The Directory: Authentication Framework (including all amendments), which is expressly incorporated here by reference. The infrastructure and certificate definitions used in this application are based on these documents.

As described below, the public/private key is advantageously delivered in the form of a Token such as an electronic circuit card conforming to the standards of the PC Memory Card Interface Association (a PCMCIA card or PC Card) for use in the originator's computer. In general a Token is a portable transfer device that is used for transporting keys, or parts of keys. It will be understood that PC Cards are just one form of delivery mechanism for public/private keys for Applicant's DAS; other kinds of Tokens may also be used, such as floppy diskettes and Smart Cards. To ensure reliable delivery a service such as the bonded courier services commonly used to ferry securities between parties could be used to deliver the media to the document originator.

Advantageously, many commercially available Tokens that embody onboard cryptography generate the public/private key pairs on the cards, and the private keys never leave the cards unencrypted. The public keys are exported to the Certification Authority for inclusion, with the identity of the intended recipient and appropriate user attributes among other things, into a "certificate". Principal components of the DAS system assurance are the correct operation of the Certification Authority framework, the tight binding of user identity and attributes to the public key in the certificate, and the reliable delivery of the Token to the authorized recipient.

In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered

5

separate from the originator's card. Any subsequent transmitter of the document who is required to digitally sign or encrypt the document would similarly be provided with a respective card and personal identification information.

In FIG. 1, a document's originator and any subsequent transmitter are called a Transfer Agent, and it will be appreciated that a Transfer Agent is identified to the DAS by its possession and use of a valid certificate and a valid PIN. In issuing the key and PIN to the Transfer Agent, the DAS advantageously records one or more attributes of the Transfer Agent in association with the key and PIN. For example, the Transfer Agent may be authorized to conduct only certain types of transactions and/or transactions having less than a predetermined value.

Issuance by the Certification Authority of a digitally signed certificate ensures the verifiability of the identity of each transmitter of a digitally signed or encrypted document. The Certification Authority also retains the ability to revoke a public/private key, or to reissue a public/private key, from a remote location electronically. The Certification Authority can also support privilege management in accordance with the policy set for the system. For example, the Certification Authority can set financial or other limits on the authority granted to the Transfer Agent by conveying those authorizations or restrictions as certificate attributes. These attributes can be retrieved from the certificate and enforced by other elements in the system.

In an important aspect of Applicant's invention, the DAS is a system for authenticating a document by applying digital signature encryption technology. As used here, "authentication" is the corroboration and verification of the identity of the party which executed, sealed, or transmitted the original document and verification that the encrypted document received is the document sent by that party. The DAS uses an Authentication Center to provide an audit or evidence trail, for applications that require this capability, from the original execution of the executed or encrypted or sealed document through all subsequent transmissions.

The Certification Authority would use a physically secure facility that is a "trusted center" having twenty-four-hour security, an alarm system, and "vaulted" construction. In view of its importance, a facility would advantageously include two-person controls, with no single person having access to key generating or key management systems. All personnel connected with the operations of cryptographic key management and transmission of electronic documents would have their trustworthiness evaluated in the surest ways possible, e.g., personal interviews, background checks, polygraphs, etc. Moreover, the Certification Authority management would implement procedures that prevent single-point failures, requiring collaboration for compromise to take place. In this way, one individual would be prevented from obtaining complete access to key generation and to key management.

Another aspect of Applicant's DAS authentication that is in contrast to prior systems is the utilization of an integrity block and a date and time "stamp" on each transmitted document. Suitable time and date stamps are those provided by systems described in U.S. Pat. No. 5,136,646 and U.S. Pat. No. 5,136,647 to Stuart A. Haber and W. S. Stornetta, Jr., both of which are expressly incorporated here by reference, and commercially available from Surety Technologies, Inc. The integrity block, i.e., the digital signature, and the date and time stamp, which are applied by the Authentication Center, eliminate the possibility of unauthorized alteration or tampering with a document by the

6

signatories subsequent to its original execution or sealing. The Authentication Center's integrity block for a document received from a Transfer Agent is generated using any of several known digital hashing algorithms. This integrity block ensures that the document cannot be altered without detection. In addition, use of the digital signing algorithm by the Authentication Center can advantageously provide for non-repudiation, i.e., precluding the originator from disavowing the document. Applicant's combination of the integrity block, date and time stamp, and audit provide notice and evidence of any attempt at alteration or substitution, even by a document's originator when the alteration is attempted after origination.

In accordance with Applicant's invention, each transaction and its documents are authenticated by transmission to the Authentication Center from the Transfer Agent's terminal. As described below, the Transfer Agent provides the document in digital form, such as the output of a conventional word processor, to the Transfer Agent's Token. As an option, a device for digitizing a hand-written signature may also be provided and the digitized signature may be added to the digital document. The digital document is digitally signed and/or encrypted by the DAS Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (e.g., by modem or computer network). Other ways of communicating the digitally signed or encrypted documents might be used (for example, dispatching a diskette containing the document), but the great advantage of electronic communication is speed.

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. The combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Applicant's invention provides for authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity.

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication as described above and stores the authenticated documents for transmission to and on behalf of authorized parties whose identities and policies are similarly authenticated by the Authentication Center. Authorization for access may be restricted to the level of a single document or group of documents.

In accordance with Applicant's invention, the DAS verifies and ensures that documents that have been transmitted, stored, or retrieved have not been accidentally or intentionally modified. The DAS can verify at any stage and at any time that a document is exactly, to the last bit, the document which was executed and transmitted by the originator and that the document has not been altered or impaired in any manner. This element of integrity combined with a digital

signature and a date and time stamp enable the DAS to ensure that a document is not a fabrication, forgery, impersonation, or unauthorized replacement of a document originally executed or sealed by the document's originator.

Since originators of documents to be signed and/or encrypted, such as loan and mortgage documents, commercial paper and other securities, property deeds and leases, etc., should be able to execute their transactions from a variety of locations, the DAS moves the heart of the cryptographic process to a Token entrusted to a respective authorized Transfer Agent. This permits individual utilization of any DAS enabled computer in any location that is networked or connected with the Authentication Center. As described above, the cryptographic cards and certificates are issued and monitored by the Certification Authority. Certificates are further controlled through the inclusion of an "expiration period" field, which enables the periodic replacement if desired of the Transfer Agent certificates. It will be appreciated that certificates in accordance with X.509 include a plurality of such fields, but only those fields important to understanding the operation of the invention are described here.

FIG. 2 summarizes the functions of the DAS relating to document transmission authorization and protection. In the left column are the functions of a Transfer Agent's Token; in the center column are other functions carried out by the Transfer Agent's transmission device; and in the right column are functions of the DAS. FIG. 3 is a diagram illustrating interconnections among three Transfer Agent terminals and a server subsystem and backup subsystem in the Authentication Center in the DAS architecture. FIG. 4 is a block diagram of the functional interrelationship between a Transfer Agent and the Authentication Center.

The cryptographic card includes components, such as a microprocessor and electronic memory devices, for carrying out the steps of a PKC algorithm as well as a symmetric encryption algorithm such as DES. Also, the card should be tamper-proof, which can be assured by designing it to delete critical keys and/or algorithms upon any attempted penetration or alteration. The National Institute of Standards and Technology has been chartered to certify the authentication implementation of the cryptographic card suppliers that may be used by the DAS.

In accordance with Applicant's invention, each transaction and its documents are authenticated using a public key contained in the Transfer Agent's certificate. Privacy, signature, and/or integrity devices and software are commercially available from a number of sources, including RSA Data Security, Inc.; Public Key Partners; Surety Technologies, Inc.; Ascom Tech AG, Switzerland; National Semiconductor; Northern Telecom Ltd.; and Spyryus.

The Authentication Center makes use of its own secret key to sign again the transaction in a manner that cannot be repudiated. The combination of the Transfer Agent's and Authentication Center's signatures (in conjunction with the physically protected audit trail) can be used at a future date to prove conclusively that an agent, employee, or firm (the Transfer Agent) initiated a specific transaction. In addition, a Notary Public support function is available for implementation as described below.

Employee or agent sign-on at the Transfer Agent's terminal is protected by the personal identification information and the cryptographic features of the cryptographic card held by that Transfer Agent. The combination of these controls uniquely identifies the agent or employee, thereby enabling DAS. In addition, agent or employee authorization

and attribute information may be stored in the certificates or Token memory in protected or sealed form as described above. The DAS uses this information in conjunction with the PIN to set privilege, access, volume and fund amount limits.

The DAS provides a distributed validation capability using a "signature" that cannot be repudiated. The strategy uses PKC to reduce the key management overhead and to provide a digital signature that cannot be repudiated for all documents and transactions. Encryption is used to provide confidentiality protection of the PIN and other transaction details as described above. These control functions of the DAS are summarized in FIG. 5.

Additionally, the DAS is compatible with the full range of modern distributed, and client/server transactional based applications. It operates effectively in LAN, WAN, and dial-up networks. The DAS preferably utilizes modern database tools, and thus the server can advantageously utilize relational technology with a SQL interface (e.g., SYBASE).

As illustrated in FIG. 4, the originator of an electronic document or other Transfer Agent may implement the DAS with a typical 486 desktop or laptop computer having the DAS encryption subsystem (Token) installed and optionally an electronic digital signature pad for hand-signed "execution" of the document. It is not required for the function of the DAS to have a hand-signed instrument since a digital signature on the document is sufficient. However, at this time, a typical party in loan or other commercial transactions requires the comfort of receiving laser-printed copies of documents which have been executed by hand. Other components and software typically provided in the Transfer Agent terminal are a communication subsystem for handling transmission of encrypted or digitally signed documents to the Authentication Center by a modem telephone line or other suitable communication link, a Token interface, a message handler, input/output interface, and multimessage input application.

The Authentication Center is advantageously organized as a server subsystem, a crypto backup subsystem, and storage. As part of the server subsystem, which may be implemented with a 486 computer running under a UNIX-type operating system, a terminal communication subsystem includes a multiprotocol controller (see also FIG. 3) that handles communications with the Transfer Agent terminals. Also provided in the server subsystem are a cryptographic key management subsystem, a backup subsystem, a relational database management system, input/output (I/O), system administration, and audit subsystem. A Token Card and backup communication subsystem interfaces with the backup subsystem mentioned above that may be implemented as a 486 computer running under a DOS-type operating system. A storage communication subsystem interfaces with the document storage device or devices mentioned above.

The DAS also would permit a "Notary Public" type of secondary support function. This would permit a third party present at the document's execution to also have a cryptographic card which would "seal" the transaction for further verification that the parties executing or sealing the document to be signed were in fact the proper parties. This additional notary function is not required, but would assist in the further authentication of the identities of the parties.

FIGS. 6a, 6b are diagrams illustrating a typical application of the DAS in the mortgage finance industry with a title company/closing agent for the loan as a Transfer Agent. In step 1, the Certification Authority completes code generation and issues Tokens to authorized parties for transferring

documents and establishing legal evidence trails. The parties, who would generally not be individuals but commercial and financial institutions such as a BANK/Mortgage Co. and a Title Co./Closing Agent, would be equipped to transmit and receive documents electronically. In step 2, a Bank/Mortgage Co. loads and electronically transmits loan documents to the Authentication Center, which forwards them to a Title Co./Closing Agent after adding integrity blocks and date and time stamps. In step 3, the Authentication Center transmits the authenticated loan documents to the Title Co./Closing Agent.

In step 4, the Title Co./Closing Agent has the documents executed by digitized autograph signature by a Homebuyer/Homeowner. In step 5, the Title Co./Closing Agent provides Homeowner/Homebuyer with "hard copies" of the signed documents. In step 6, the Title Co./Closing Agent transmits the documents to the Authentication Center, which adds the integrity blocks and dates and time stamps the executed documents, forwards the documents to the Bank/Mortgage Co., and stores the documents. Whenever the Bank/Mortgage Co. needs copies of the authentic documents, they can be retrieved on-line from Authentication Center storage.

In step 7, the Bank/Mortgage Co. directs that the authentic documents be transferred by the Authentication Center to a secondary-market Mortgage Bank/Investor. In step 8, whenever the Investor needs authentic documents, they can be retrieved on-line from the Authentication Center.

FIG. 7 further illustrates an example of Applicant's document certification process. In the first step, an electronic document is designed, or drafted, that reflects the agreement of parties, such as a manufacturing operation depicted by the factory in FIG. 7. The electronic document is provided to a Transfer Agent's terminal, which is illustrated as a portable computer having an authorized Token and, optionally, a stylus pad for capturing hand-written signatures. A typical configuration for a Transfer Agent's terminal is at least the computational equivalent of a 386 desktop or laptop computer, with high resolution graphics, a Token reader, and a stylus pad for capturing hand-written signatures. As shown in FIG. 7, the electronic document, which may be created locally or remotely, is displayed on this terminal.

In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document. After all parties have signed the document, the Transfer Agent certifies the completion of the document's execution by invoking his or her digital signature and appending his or her certificate, using the Token.

If an original paper document were desired, the electronic document would be printed first. The paper document would then be placed on the stylus pad and the terminal's cursor positioned to the corresponding place in the electronic document. This permits the capture and transfer of hand-written signatures during the actual signing of the paper document. The electronic version is then an exact duplicate of the paper document.

After local certification, the Transfer Agent transmits the electronic document to the Authentication Center in the third step of the process. The Authentication Center preferably includes a high-volume utility server computer, having substantial storage capacity and backup capability, and is a secure and highly assured facility. The Authentication Center contains a separate digital signature capability, one or more Tokens, and an accurate time base.

When an electronic document is received, the authenticity and rights of the Transfer Agent are validated by the Authen-

tication Center (step 4). If authenticated, the electronic document is time- and date-stamped (step 5), digitally signed (step 6), journaled (step 7), and stored by the Authentication Center. Certified copies of the electronic document may then be distributed according to instructions from an appropriate party, such as the holder of a beneficial interest (owner) designated by the document.

The Authentication Center maintains the electronic document and a log, or history, of all transactions, such as requests for copies, etc., related to it. It will be appreciated that the log is useful for many management functions that contribute to the usefulness of the system. For example, the log facilitates identifying subsequent electronic submissions related to a transaction and contributes to liability limitation for the Authentication Center. Also, the log is useful as evidence of the document's chain of custody.

The Authentication Center also controls access to the document in accordance with authorization instructions provided by the owner of the document. Such authorization instructions would be updated or revised in conformance with changes (e.g., assignments) in the document's ownership.

FIG. 8 illustrates the process of digitally signing an electronic document, depicted more generally as an "information object", by application of a hash function. In general, a hash function is a truly one-way cryptographic function that is computed over the length of the information object to be protected. The hash function produces a "message digest" in a way such that no two different information objects produce the same message digest. Since a different message digest is produced if even one bit of the information object is changed, the hash function is a strong integrity check.

In accordance with the invention, the message digest is encrypted using the signatory's secret key, thereby producing the signatory's digital signature. The combination of hashing and encryption in this way insures the system's integrity (i.e., the ability to detect modification) and attribution capability (i.e., ability to identify a signatory, or responsible party). The digital signature (the encrypted message digest) is appended to the readable information object (see steps 2 and 6 depicted in FIG. 7).

Of the many different hash functions that are known, it is currently believed that those designated MD4 and MD5, which are embodied in circuits commercially available from vendors identified above, and the U.S. government's published secure hash algorithm are suitably robust for use in Applicant's DAS. Of course, other hash functions can be expected to become available as time passes.

The steps of digitally signing an electronic document (steps 2 and 6 depicted in FIG. 7) and validating the digital signatures (step 4 in FIG. 7) are further illustrated in FIG. 9. The electronic document has appended to it one or more digital signatures, which are created by using a signature algorithm and the secret key(s) of the signatory(s) as described in connection with FIG. 8, and the certificate(s) of the signatory(s). As described above, each such certificate conveys the identity of the signatory, the signatory's public signature/verification key, predetermined collateral information about the signatory, and the digitally signed message digest of the certificate. The format of these pertinent parts of such a certificate in accordance with the X.509 Recommendation that would be employed by a user or the Certification Authority is illustrated in FIG. 10.

The signature validation step, which would normally but not necessarily be carried out by the Authentication Center, comprises decrypting the message digest appended to the

document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document.

As shown in FIG. 11, a certificate of a user (Transfer Agent) or even of a Certification Authority is preferably digitally signed in substantially the same way that electronic documents are digitally signed, except that such a certificate is signed by authorities specifically empowered to create certificates. Validation of a document's digital signatures includes validation of the public signatures of all Certification Authorities in a path between the signatory and a Root Authority, which is the most superior Certification Authority. The signatures of these Certification Authorities are loaded in the signatory's Token and appended to documents prepared with that Token.

As illustrated by FIG. 12, the path from the signatory to the Root Authority may be considered part of an authentication tree. The signatory's (user's) certificate is digitally signed by a Certification Authority whose own certificate (the CA Certificate) is signed by the Root Certification Authority. Since there is likely to be a plurality of Certification Authorities located on different branches of the authentication tree, it is only necessary to retrieve all Certification Authority certificates along both branches until a common node is encountered, in order to authenticate a digital signature for an entity on a different branch of an authentication tree, and to verify the authenticities of the certificates up to the common node.

It will be noted that the present description and drawings are illustrative only and that one of ordinary skill in the art would recognize that various modifications could be made without departing from the spirit or scope of the present invention which is to be limited only by the following claims.

What is claimed is:

1. A method of authenticating an electronic document, comprising the steps of:

signing the electronic document with a digital signature of a transfer agent;

appending a certificate to the electronic document by the transfer agent, wherein the certificate relates a cryptographic key to an identity of the transfer agent;

applying a date stamp and a time stamp to the electronic document;

validating the digital signature and certificate of the transfer agent;

signing the electronic document with a second digital signature and appending a second certificate to the electronic document signed with the second digital signature after the digital signature has been validated, wherein the second certificate relates a cryptographic key to the second digital signature; and

storing in a facility identified by the second digital signature, the document signed with the second digital signature and having the second certificate appended such that the facility assumes control of the document.

2. An apparatus for authenticating an electronic document, comprising:

means for signing the electronic document with a digital signature of a transfer agent;

means for appending a certificate to the electronic document, wherein the certificate relates a cryptographic key to an identity of the transfer agent;

means for applying a date stamp and a time stamp to the electronic document;

means for validating the digital signature and certificate;

means for signing the electronic document with a second digital signature and for appending a second certificate to the electronic document signed with the second digital signature after the digital signature has been validated by the validating means, wherein the second certificate relates a cryptographic key to the second digital signature; and

means, identified by the second digital signature, for storing the document signed with the second digital signature and having the second certificate appended such that the storing means assumes control of the document.

3. A method of executing a transaction by transferring an authenticated information object having a verifiable evidence trail, comprising the steps of:

signing, by a first entity, the information object with a first digital signature;

appending, by the first entity, a first certificate to the information object, wherein the first certificate relates at least an identity and a cryptographic key to the first entity;

authenticating the information object signed with the first digital signature and having appended the first certificate by a second entity, thereby forming an authenticated object, wherein the step of authenticating comprises:

validating the first digital signature and first certificate;

applying a date stamp and a time stamp to the information object signed with the first digital signature and having appended the first certificate; and

after the validating and applying steps, taking control of the validated stamped information object by signing the information object with a second digital signature of the second entity, appending a second certificate to the information object, and storing the validated stamped information object signed with the second digital signature and having the second certificate appended as the authenticated object, wherein the second certificate relates at least an identity and a cryptographic key to the second entity; and transferring the authenticated object to an entity in response to an instruction.

4. The method of claim 3, wherein the transferring step comprises retrieving the stored authenticated object and providing the retrieved authenticated object to the entity in accordance with the instruction.

5. The method of claim 4, wherein the retrieved authenticated object is provided to each of a plurality of entities in accordance with the instruction.

6. The method of claim 3, wherein each signing step comprises the steps of applying a hash function to the information object to determine a message digest and using the message digest with a secret cryptographic key of the respective one of the first and second entities to determine the respective digital signature.

7. The method of claim 6, wherein the validating step comprises the step of using the digital signature with a public cryptographic key of the first entity, and with another

13

message digest determined by applying the hash function to the information object.

8. The method of claim 3, further comprising the step of maintaining a log relating to the authenticated object so as to identify at least one subsequent information object related to the transaction. 5

9. The method of claim 8, wherein a subsequent information object is signed by a third digital signature of a third entity.

10. An apparatus for executing a transaction by transferring an authenticated information object having a verifiable evidence trail, comprising:

first means for signing, by a first entity, the information object with a first digital signature and for appending, by the first entity, a first certificate to the information object, wherein the first certificate relates at least an identity and a cryptographic key to the first entity; and 15

means for authenticating an information object signed with the first digital signature and having appended the first certificate by a second entity, thereby forming an authenticated object, wherein the authenticating means comprises:

means for validating the first digital signature and first certificate;

a date stamp and a time stamp for application to an information object signed with the first digital signature and having appended the first certificate; and 25

means for controlling a validated stamped information object, wherein the controlling means comprises second means for signing an information object with a second digital signature of the second entity and for appending a second certificate to the information object, and a memory;

wherein the memory includes storage locations for validated stamped information objects signed with

14

the second digital signature and having the second certificate appended as authenticated objects, an authenticated object stored in the memory is transferable in response to an instruction, and the second certificate relates at least an identity and a cryptographic key to the second entity.

11. The apparatus of claim 10, wherein each signing means comprises a processor for applying a hash function to the information object to determine a message digest and for using the message digest with a secret cryptographic key of the respective one of the first and second entities to determine the respective digital signature.

12. The apparatus of claim 11, wherein the signing means is an electronic circuit card.

13. The apparatus of claim 11, wherein the validating means comprises a processor for using the digital signature with a public cryptographic key of the first entity, and with another message digest determined by applying the hash function to the information object.

14. The apparatus of claim 10, wherein an authenticated object is transferred in response to the instruction by retrieving the authenticated object from the memory a plurality of times and providing the retrieved authenticated objects to a plurality of entities.

15. The apparatus of claim 10, wherein the authenticating means further comprises a log relating to authenticated objects and identifying at least one subsequent information object related to the transaction and stored in the memory. 30

16. The apparatus of claim 15, wherein a subsequent information object is signed by a third digital signature of a third entity.

* * * * *

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any related appeals, interferences or judicial proceedings.